

الحرب الإلكترونية

د. فيصل محمد عبد الغفار

الجنادرية للنشر والتوزيع
ALJANADRIA

الحرب الإلكترونية

د.فيصل محمد عبدالغفار

الطبعة الأولى 2016



ISBN: 978-9957-580-75-9

المملكة الأردنية الهاشمية

رقم الإيداع في المكتبة الوطنية

2015/10/4972

355.07

إسم الكتاب: الحرب الإلكترونية

إسم المؤلف: فيصل محمد عبدالغفار

الواصفات: العلوم العسكرية//الحرب الالكترونية/



الأردن- عمان

جوال: 962796296514

تلفاكس: 96264778770

ص.ب 520651 عمان 11152 الاردن

E-mail: dar_janadria@yahoo.com

المقدمة

يُعَدُّ ظهور ثورة تكنولوجيا الإلكترونيَّات واستخدامها في الأغراض العسكرية - نقطة تحوُّل كبيرة؛ سواء في فنِّ الحرب، أو في إدارة الصراع المسلَّح، فقد أخَذت أسلحة القتال الحديثة ومعداته مكان الصدارة في حسْم أيِّ صراعٍ مسلَّحٍ، وخاصة أسلحة الهجوم الجوي الحديثة؛ لاعتمادها على نُظم السيطرة والتوجيه الإلكتروني، التي تمكِّنها من تنفيذ المهام المطلوبة منها بكفاءة، وإصابة أهدافها بدقَّة عالية؛ نظرًا لاستخدامها نُظُمَ ووسائل الكشْف والتوجيه والتحكُّم، وقيادة النيران وتصحيحها لاسلكيًّا، ورادارِيًّا، وحراريًّا، وليزريًّا، وتليفزيونيًّا، وهي النُّظم التي يستوي تشغيلها واستخدامها ليلاً ونهارًا، هذا إضافة إلى النُّظم الحديثة والمتقدِّمة للتصوير التليفزيوني باستخدام آلات التصوير ذات الحساسية العالية، التي يُمكنها العمل في مستوى الضوء المنخفِض بكفاءة ودقَّة عاليتَيْن.

كانت أساليب الحرب الإلكترونيَّة تستعمل منذ بداية هذا القرن، وبالأخص عندما استُخْدِمت أجهزة الاتِّصالات اللاسلكية في الحروب، ولكن منذ الحرب العالمية الثانية أصبَح موضوع الحرب الإلكترونية محلَّ الاهتمام، من حيث المعدات والأساليب.

تفيد المصادر أن أوَّل عمليَّة في مجال الحرب الإلكترونية كانتْ في عام 1905م خلال الحرب الروسية اليابانيَّة في معركة (tsushima)، عندما كانت سُفن الاستطلاع اليابانية تُراقب الأسطول الروسي عن كثبٍ، وتُرسل جميع المعلومات بالراديو إلى القيادة الرئيسية اليابانية، وفي هذه الأثناء الْتَقَط أحد قادة الزوارق الروسيَّة هذا الإرسال، فطلب الإذنَ باستعمال جهاز الإرسال الموجود

بزورقه؛ لإعاقة تلك الإرساليات، ولكنَّ طلَبَه قُوبِلَ بالرفض من قِبَل القيادة الروسية، فاستمرَّ إرسال المعلومات الروسيَّة، وبعد فترةٍ وجيزةٍ استطاعَ أحد قادة الزوارق الروسيَّة - دون إذنٍ مِن قيادته - التشويشَ على هذه الإرساليات، ولكن بعد فَوَات الأوان؛ إذ كانت المعركة قد وقَعَت وخَسِرها الروس!

أمَّا في الحرب العالميَّة الأولى، فقد استُعْمِلَت أجهزة الاتِّصالات وأجهزة نقْل معلومات الاستطلاع بكثرة؛ إذ استطاعَت إحدى السفن الإنجليزية عام 1914م أن تُرسل بالراديو معلومات عن تحرُّك بعض القطَع الحربية الألمانيَّة في البحر الأبيض المتوسط، ولكن بعد أن رصَد الألمان تلك الإرساليات، تمكَّنوا من التشويش الكامل عليها.

وفي عام 1916 وضَع الإنجليز بعض موجدات اتجاه الإرسال قُرب الأسطول الألماني، وخلال معركة" جوتلاند "حدَّدت تلك الأجهزة موقع الأسطول، وأبْلَغَت القيادة الإنجليزية بذلك.

كانت البداية الحقيقيَّة في الحرب العالمية الثانية لاستخدام أجهزة الحرب الإلكترونيَّة المتخصِّصة، ففي عام 1939م استخدم الألمان طريقة تقاطُع موجات الإرسال فوق الهدف (beam-intersection)؛ لكي يقصفوا المدن الإنجليزيَّة، وخاصة أثناء الليل، فوضَع الإنجليز جهاز الإرسال (bromide)؛ ليقوم بتشويش مخادع، ويجعل هذا التقاطع فوق مكان غير حيوي، واختاروا لذلك بحر" المانش"، وفعلاً وقَع قصْف الطائرات الألمانيَّة على بحر" المانش"، ولَم تتضرَّر المُدُن الإنجليزية التي أراد الألمان قصْفها!

ليس هناك من إجماع واسعٍ على تعريـف محـدَّد ودقيـق لمفهـوم الحـرب الإلكترونيـة الآن، وعلى الرغم من ذلك، فقد اجتهَد عدد من الخُـبراء ضـمن اختـصاصاتهم في تقـديم تعريـفٍ يُحيط بهذا المفهوم:

يعـرِّف مـصطلح الحـرب الإلكترونيـة بأنهـا: "مفهـوم يـشير إلى أيٍّ نـزاع يحـدث في الفـضاء الإلكتروني، ويكون له طابع دولي."

أو "هــي مجموعــة الإجـراءات الإلكترونيَّــة المتــضمنة اســتخدامَ بعــض الــنُّظم والوســائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نُظم العـدو ووسـائله ومعداته الإلكترونيَّة المختلفة، مع الاستخدام المتعمَّـد للطاقـة الكهرومغناطيـسية في التـأثير عــلى هــذه الــنُّظم والوســائل؛ لمنــع العــدو أو حِرمانــه، أو تقليــل اســتغلاله للمجــال الكهرومغناطيسي، فضلاً عن حماية الموجات الكهرومغناطيسيَّة الصادرة من النُّظم والوسائل الإلكترونيَّة الصديقة من استطلاع العدوِّ لها، أو التأثير عليها."

وسوف نتناول في كتابنا هذا مفهـوم الحـرب الألكترونيـة ودراسـة آثارهـا وفوائـدها للدولـة والمجتمع في حال السلم والحرب.

ونسأل الـلـه التوفيق وأن يكون عملاً خالصاً لوجهه تعالى

المؤلف

الفصل الاول

مفهوم وأهداف الحرب الألكترونية

مقدمة عامة

كما البر والبحر والجو والفضاء، دخل المجال الإلكتروني على ما يبدو ميادين الحروب، حيث من المتوقع أن تكون الحرب الإلكترونية (Cyberwar) السمة الغالبة إن لم تكن الرئيسة للحروب المستقبلية في القرن الواحد والعشرين.

وتكمن خطورة حروب الإنترنيت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني (Cyberspace) لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الإلكترونية والتي نشهد جزءًا بسيطا منها اليوم يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكومبيوتر والإنترنيت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل، علما أنّ أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وحتى العامة.

نحاول من خلال هذه الورقة التطرق لمفهوم الحرب الإلكترونية من ناحية أنواعها وخصائصها والمجالات التي تستهدفها إضافة إلى مخاطرها والتطورات التي تشهدها الساحة العالمية على هذا الصعيد.

مفهوم الحرب الإلكترونية

ليس هناك من إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية الآن. وعلى الرغم من ذلك، فقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم

في تقديم تعريف يحيط بهذا المفهوم، فعرّف كل من "ريتشارك كلارك" و"روبرت كناكي" الحرب إلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.

فيما يعرّف آخرون مصطلح الحرب الإلكترونية بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي". ولأن مثل هذه التعريفات فضفاضة ولا تعبّر بدقّة عن فحوى الموضوع، يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء الإلكتروني، ومنها:

- القرصنة الإلكترونية: أو التخريب الإلكتروني، وتقع في المستوى الأول من النزاع في الفضاء الإلكتروني، وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء المحتوى. ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة أو ما يعرف باسم الملقّمات (Servers) من خلال إغراقها بالبيانات.

- الجريمة الإلكترونية والتجسس الإلكتروني: ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.

- الإرهاب الإلكتروني: ويقع في المستوى الرابع من النزاع في الفضاء الإلكتروني. ويستخدم هذا المصطلح لوصف الهجمات غير الشرعية التي تنفّذها مجموعات أو فاعلون غير حكوميون (Non-State Actors) ضد

أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة. ولا يمكن تعريف أي هجوم إلكتروني بأنه إرهاب إلكتروني إلا إذا انطوى على نتائج تؤدي إلى أذى مادّي للأشخاص أو الممتلكات والى خراب يترك قدرا كبيرا من الخوف.

- الحرب الإلكترونية: وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني، وتعتبر جزءا من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني.

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

- حروب الإنترنيت هي حروب لا تناظرية (Asymmetric): فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال.

- تمتّع المهاجم بأفضلية واضحة: في حروب الإنترنيت يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة، من الصعب جدا على عقليّة

التحصّن لوحدها أن تنجح. فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط.

- فشل نماذج "الردع" المعروفة: يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحـرب الباردة غير ذي جدوى في حروب الإنترنيت. فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب. فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ مـن أمـاكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بـل ومـن المـستحيل في كثـير مـن الأحيـان تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحـالات قـد تتطلّـب أشـهرا لرصـدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكـن تتبـع مـصدرها في المقابـل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فانه في هـذه الحالـة لـن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

- المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار حروب الإنترنيـت باسـتهداف المواقع العسكرية، فهناك جهـود متزايـدة لاسـتهداف البنـى التحتيـة المدنيـة والحـسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيا في ظل القـدرة عـلى اسـتهداف شـبكات الكهربـاء والطاقة وشبكات النقل والنظام المالي والمنـشآت الحـساسة النفطيـة أو المائيـة أو الـصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.

وتشير العديد من التقارير إلى تزايد أعداد الهجـمات الإلكترونيـة التـي تـتم في العـالم اليـوم والتي تقوم بها مجموعـات أو حكومـات تتـدرج في الاسـتهداف مـن أبـسط المـستويات إلى أكثرها تعقيدا وخطورة.

ففي ديسمبر/كانون الأول من العام 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفّذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.

وفي يوليو/ تموز 2010، أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.

ويجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف أستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسببا خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من أنّ الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف أستوني- روسي كبير، إلا أنّ أحدا لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الإنترنيت إلى الآن.

ملامح الحرب الإلكترونية

يظن كثيرون أن مصطلح الحرب الإلكترونية هو أحد المصطلحات التي تتحدث عن مفهوم افتراضي تدور تفاعلاته في فضاء الإنترنت، ولكن هذا التصور يعتبر تصورا خاطئا إلى حد بعيد، فالإنترنت وشبكات الحاسب بوجه عام تعتبر

أحد ميادين الحـرب الإلكترونيـة التـي فاقـت أسـلحتها في القـوة التدميريـة قـدرة الأسـلحة التقليديـة وفـوق التقليديـة. فـالحرب الالكترونيـة هـي الأعـمال المتخـذة لتحقيـق الـسبق والأفـضلية المعلوماتيـة عـن طريـق التـأثير عـلى معلومـات العـدو وأنظمتهـا والـدفاع عـن المعلومات الخاصة وأنظمتها.

ويحفل واقع اليوم بالعديد من المتغيرات التي تـدفعنا إلى تـسليط الـضوء عـلى تلـك الآلـة العسكرية الجديدة، التي فرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة في عالم اليوم.

لقد زادت التقنيات الرقمية من فاعلية الحروب الالكترونيـة، فكـان أول إعـلان عـن دخـول التقنيات الرقمية ميادين الحروب في حرب البلقان في نهايات القرن المـاضي عـلى يـد حلـف الناتو ضد الصرب فيما سمي "بالقنابل المعتمة"، وقد أدى هذا الهجوم الإلكتروني إلى توقـف شبكة الحاسب الرئيسية مما أصـاب نظـم الكمبيـوتر الخاصـة بـوزارة الـدفاع اليوغـسلافية بالشلل التام.

واستطاعت القنابـل الإلكترونيـة تعطيـل الاتـصالات عـبر التـشويش عـلى شـبكة الاتـصالات الهاتفية الرئيسية "الثابتة" مما دفـع القيـادة في بلجـراد إلى الاتـصال بقواتهـا عـبر الهواتـف الجوالة وبالتالي أصبح يسيرا على قوات الحلف مهمة اختراق المكالمات.

ويمكــن تلخــيص مهمــة القنابــل الإلكترونيــة في تنفيــذ عــدد مــن المهــام الاســتراتيجية مثـل تعطيـل الاتـصالات والتـشويش عليهـا والتنـصت عـلى المكالمـات، وبـث معلومـات مــضللة عــبر شــبكات الحاســب والهــاتف، ومنهــا تقليــد بــصمات الأصــوات

وخاصة أصوات القادة العسكريين وعن طريق ذلك يمكن إصدار أوامر ضارة بالقوات، واستهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات ومسح الذاكرة الخاصة بالأجهزة المعادية، ومنع تدفق الأموال وتغيير مسار الودائع، وإيقاف محطات الكهرباء عن العمل وقد صممت لذلك قنبلة إلكترونية خاصة أطلق عليها اسم: "cbu94" تنطلق منها عدة قنابل في الجو وتستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها بالكامل.

وفي حرب الخليج الثانية تم ابتكار العديد من الأسلحة الهجومية الإلكترونية وخاصة تلك المعتمدة على الطاقة الموجهة الحديثة -ومنها أسلحة الميكروويف عالية القدرة high-power microwave weapons المعروفة اختصارا بـ "إتش بي إم" (HPM)- من أهم الأسلحة الجديدة في مجال الحرب الإلكترونية، ويمكن استخدامها لاختراق الأهداف عالية التحصين لتدمير و"شل" أسلحة الدفاع الجوي والرادارات وأجهزة الاتصال والحاسبات التي تعمل ضمن منظومة القيادة والسيطرة. كما يمكنها تدمير أجهزة التحكم في إنتاج وتخزين المواد الكيماوية والحيوية.

ووفقا للخبراء، فإن هذه الأسلحة تنتج شحنات عالية من الطاقة التي تؤدي للإضرار بالأدوات الإلكترونية وتقوض ذاكرة الحواسب، وتتميز بالدقة الشديدة في إصابة الهدف.

ويمتاز الواقع العربي في هذا المضمار بثلاثة سمات أساسية، أول ملامحها تلك الفجوة التقنية التي تعبر عن نفسها بذلك التنافس العربي الملحوظ نحو "شراء" وسائل الحرب الإلكتروني، وليس تطويرها، سواء فيما يتعلق بالشق الدفاعي أو

الهجومي، بما يعني بقاء المجتمعات العربية "تحت السيطرة " التقنيـة الكاملـة حيـث يبيـع الآخرون للعرب تقنيات إما عفـا عليهـا الـزمن أو ظهـر مـا يفوقهـا تـدميرا. كـما أن الـسلاح التقليدي وعند اقتنائه فمن الممكن الاستفادة منه كما يريد من اقتناه، وعـلى النقـيض فـإن أدوات الحرب الإلكترونية فمن الممكن تعطيلها بشكل أو بآخر أو تـضليلها في الوقـت الـذي يريده البائع

أما ثاني هذه الملامح فهو انحسار مفهوم الحرب الإلكترونية ليقتصر على مـا يـسميه الـبعض بالجهاد الإلكتروني أو الإنترفاضة، ويقصد به محاولة تـدمير مواقـع الـشبكة الخاصـة بـبعض الجهات التابعة للأعداء بأساليب تقنية معينة. وقـد انطلقـت الحـرب الإلكترونيـة بمفهومهـا هذا ضد إسرائيل في منتصف أكتوبر مـن العـام2000 م، حيـنما قامـت مجموعـة إسرائيليـة بتخريب موقع حزب اللـه بعد قيام الحزب بأسر الجنود الإسرائيليين الثلاثة في جنوب لبنان

ووفقاً لإحصاءات شركة آي ديفنس (eye defense)الأميركية المتخصصة في أمـن المعلومـات، فقد بلغت حصيلة المواقع الإسرائيلية التي تم تدميرها أو اختراقها حتى 15 من يناير 2001م هي 246 موقعاً مقابل 34 موقعـاً عربيـاً اخترقـه أو دمـره مؤيـدون لإسرائيـل، والملاحـظ أن معظم الهجمات الإسرائيلية استهدفت مواقـع حكوميـة عربيـة حيويـة، ومـن بينهـا وزارات الخارجية والاقتصاد والزراعة في مصر، ووزارة الاتصالات في المغرب، وأحد البنوك السعودية.

وعــلى الــرغم مــن أن الــبعض يفــضل النظــر إلى انتــشار مفــاهيم "الجهــاد الإلكــتروني" بــشكل ســطحي، إلا أن التأمــل في نتــائج شــيوع هــذا الــسلوك يجــد أن آثــاره الــسلبية عــلى الواقــع العــربي تفــوق تلــك الآثــار التدميريــة التــي قــد يتعــرض لهــا العــدو لبــضع

ساعات، فضلا عن أن هـذا الاتجـاه سـاهم بـشكل فعـال في تـوفير خريطـة تفـصيلية لـدى إسرائيل توضح مواقع الحواسب المعادية في العـالم وقـد سـاهمت تلـك الحـروب التقنيـة في تفعيـل الأنظمـة الدفاعيـة لـدى إسرائيـل فهـي الباعـث وراء قيـام إسرائيـل بإنـشاء معهـد متخصص في تخريج خبراء تقنية وأمن المعلومات تـتراوح مهـامهم بـين الإعـداد لمواجهـة أي أخطار إلكترونية يتعرض لها أمن إسرائيل، وشن هجمات إلكترونية ضمن أي حرب تنشأ مـع العرب، وتطوير فيروسات لتدمير معلومات الحاسبات والشبكات العربية. كما أن المساهمين في تخريب المواقع الإسرائيلية بغض النظر عن نيـتهم فيتـصف أكـثرهم بالجهـل والـسطحية حيث يقوم بالمشاركة وتسخير وقته وجهازه لأي نشاط يقال أنه معادي لإسرائيل وقد يكـون من يـدير هـذا النـشاط جهـات إسرائيليـة تـستخدم الكلـمات العربيـة والجهاديـة للهجـوم المعاكس على المصالح العربية والإسلامية.

أما الملمح الثالث من ملامـح الواقـع العـربي في ميـدان الـسلاح الإلكـتروني، فيتعلـق بمناعـة أنظمتنا إلى حد ما من أي هجوم إلكتروني، ويعود الفضل في ذلك إلى التخلف التقني وعـدم الاعتماد التقنيات الحديثة والالكترونية لتطوير كفاءة الأعمال في القطاعات الخاصة والعامـة والخدمات. وإن كان هذا أمرا مفرحا في وهلته الأولى إلا أنه دلالة على ضعف فاعليـة هـذه الخدمات.

إن أفضل وقت للتحضير للحرب الإلكترونية وبنائهـا وتجريبهـا دفاعيـا وهجوميـا هـو وقـت السلم وليس وقت الحرب فهل يا ترى لدى الدول العربيـة محـاولات جـادة وذاتيـة لوضـع استراتيجيات الحرب الإلكترونية.

الحرب الإلكترونية: نشأتها، وتطورها، ومفهومها

عند تتبع تاريخ نشأة الحرب الإلكترونية في العالم، نجد أن جذورها تعود لما قبل اندلاع الحرب العالمية الأولى، فقد بدأت الاتصالات بين أرجاء العالم المختلفة باستخدام المواصلات السلكية من طريق المورس "جهاز البرق الصوتي" عام 1837؛ ولم يتحقق أي اتصال آخر في ذلك الوقت إلا من طريق تبادل المراسلات؛ باستخدام السفن في نقل الرسائل بين الموانئ البحرية.

منذ اندلاع الحرب الأهلية في الولايات المتحدة الأمريكية، في أبريل 1861، كانت خطوط التلغراف هدفاً مهماً للقوات المتحاربة؛ إذ كان عمال الإشارة يتداخلون على خطوط المواصلات السلكية، من طريق توصيل هاتف على التوازي مع كل خط من هذه الخطوط؛ للتنصت على المحادثات؛ ولهذا السبب، كان كل جانب يقطع المواصلات الخطية عند عدم الحاجة إليها، حتى لا يتداخل عليها الطرف الآخر.

ثم كانت بداية استخدام الاتصال اللاسلكي في عام 1888 مع الألماني هرتز Hertz. وفي منتصف عام 1897 استطاع "ماركوني" Guglielmo Marconi المهندس والمخترع الإيطالي من تطوير جهاز لاسلكي يناسب الاستخدام في البحر. ثم استخدم اللاسلكي في أعمال الاتصالات بالمسرح البحري الأوروبي في عام 1901.

ونتيجة لتزايد الاستخدام اللاسلكي، كان طبيعياً أن تظهر الشوشرة على الاتصالات اللاسلكية، وكانت في البداية شوشرة طبيعية، نتيجة لكثرة استخدام

الأجهزة اللاسلكية، وهو ما يعرف بالتداخل البيني للموجات الكهرومغناطيسية عند إشعاعها بكثافة عالية في مساحة محددة، أو في مناطق مغلقة، مثل المضايق والممرات الجبلية. ومن هنا بدأ التدريب على العمل في ظل الشوشرة نتيجة الاستخدام اللاسلكي المكثف، ثم بدأ الاستخدام المتعمد للشوشرة؛ لإعاقة الاتصالات اللاسلكية بين الوحدات العسكرية المعادية؛ لإرباكها وشل سيطرتها على قواتها وأسلحتها.

وفي عام 1904 قصفت السفينتان اليابانيتان الحربيتان "كاسوجا ونيشين" القاعدة البحرية الروسية في ميناء "آرثر" Arthur، وكانت معهما سفينة صغيرة تصحح النيران باستخدام الراديو "اللاسلكي"، وسمع أحد عمال "الإشارة" الروس، بالمصادفة، تعليمات تصحيح النيران، فاستخدم جهاز إرساله اللاسلكي في إعاقة الاتصال الياباني بالضغط على مفتاح الإرسال على تردد الشبكة اليابانية نفسها، مما عطل بلاغات تصحيح النيران من أن تُبّلغ لمدفعية السفينتين؛ وهكذا، لم ينتج عن هذا القصف البحري سوى إصابات طفيفة، لعدم دقة النيران في إصابة أهدافها.

وحتى عام 1905، وخلال المعارك بين السفن اليابانية والروسية، استخدمت السفن الروسية الأسلوب نفسه ضد الشبكات اللاسلكية اليابانية، وانعكس ذلك في أن السفن الروسية استطاعت إخفاء اتصالاتها، قدر الإمكان، من طريق تقليل فترات استخدام اللاسلكي لأقل فترة ممكنة، وبأقل قدرة إشعاع لاسلكي تحقق الاتصال المطلوب، وكانت السفن الروسية تتنصت وتراقب الإرسال اللاسلكي الياباني، ثم تشوّش عليه أثناء القصف بهذا الأسلوب نفسه.

وفي عام 1906 استطاع مكتب معدات البحرية الأمريكية من استحداث جهاز تحديد اتجاه لاسلكي؛ لخدمة الملاحة البحرية في البحر، وهو ما يعرف باسم "المنارة اللاسلكية" لإرشاد السفن، وتحديد مواقعها، وخطوط سيرها، مما كان له أثر كبير في مجالات الحرب الإلكترونية فيما بعد.

1. الحرب الإلكترونية في الحرب العالمية الأولى

في بداية الحرب العالمية الأولى، في أغسطس 1914، قبل أن تدخل بريطانيا الحرب إلى جانب بلجيكا وفرنسا، ضد ألمانيا، والنمسا، مرت سفينتان حربيتان بريطانيتان، بجوار السفن الألمانية في بحر المانش، ولم تحاولا الاشتباك مع السفن الألمانية. إلا أن أدميرال الأسطول الألماني "إرنست كينج"، أوضح أن هاتين السفينتين البريطانيتين، نفذتا عمليات التنصت اللاسلكي على الاتصالات اللاسلكية للسفن الألمانية، وذلك عندما حاولتا التشويش على الاتصالات اللاسلكية الألمانية، بهدف اختبار كفاءة أعمال الحرب الإلكترونية لديها في التداخل والشوشرة اللاسلكية على الشبكات اللاسلكية الألمانية.

وأثناء العمليات البحرية التالية في الحرب العالمية الأولى، كان التشويش على الاتصالات اللاسلكية يستخدم من حين إلى آخر، ولكن وُجد أنه، لكي تنفذ الشوشرة على أي اتصال لاسلكي، كان لا بد أن تسبق عملية التنصت هذا الاتصال، الأمر الذي تبين منه في أحيان كثيرة، أهمية المعلومات التي يتبادلها الجانب المعادي، والتي يمكن الحصول عليها، معرفة نواياه المستقبلية.

ومن هنا ظهرت أهمية أعمال الاستطلاع اللاسلكي على شبكات العدو اللاسلكية، بهدف الحصول على المعلومات، كما أصبحت الوحدات البحرية على دراية بأن استخدام اللاسلكي أكثر مما ينبغي، يمكن أن يفصح عن حجم كبير من المعلومات المفيدة للعدو، حتى مع استخدام الكود والشفرة في الاتصالات اللاسلكية.

ولهذا السبب، أكد القادة على أهمية بقاء الراديو "اللاسلكي" صامتاً كلما أمكن ذلك، وتقليل تبادل الإشارات إلى الحد الأدنى عندما لا يكون آمناً، أي بمجرد أن تكون السفن الحربية في مرمى بصر العدو، فكان لا يسمح للقادة باستخدام الراديو "اللاسلكي" بِحُرية حتى لا يلتقطه الجانب المعادي، وكان يستعاض عنه، في تحقيق الاتصال، باستخدام الإشارات المرئية "التأشير المنظور".

بعد ذلك ظهرت أهمية تحديد مواقع المحطات اللاسلكية المعادية، التي تدل على أماكن تمركز القوات المعادية، وبالتالي يمكن التنبؤ المبكر بالتهديد، وكذلك لتوجيه أعمال الشوشرة ضدها بدرجة تركيز مناسبة في التوقيت المناسب، ففي عام 1915، استغلّت البحرية البريطانية الفكرة الأمريكية في إنشاء جهاز تحديد اتجاه الإشعاع اللاسلكي الصادر من جهاز إرسال أي سفينة تستخدم الاتصال اللاسلكي وهي في عرض البحر، والذي يمكن باستقباله تحديد موقع هذه السفينة "نظام المنارة اللاسلكية"، وعلى ضوء ذلك، بدأت البحرية الملكية البريطانية، بتركيب سلسلة من محطات تحديد الاتجاه اللاسلكي بطول الساحل الشرقي لإنجلترا، حيث أمكنها تحديد موقع أي سفينة أو طائرة منطلقة في بحر الشمال. وعندما دخلت أمريكا الصراع في أبريل 1917، انضم الأسطول

الحربي الأمريكي مع الأسطول البريطاني، الذي كان يمتلك أجهزة لاسلكية متقدمة، وكانت بعض قطع الأسطول تحمل أجهزة تحديد اتجاه من نوع 995، أثبتت كفاءة كبيرة في تحديد مواقع السفن المعادية التي كانت تتنصت على اتصالاتها اللاسلكية، وتحدد مواقعها، وتتتبعها، ثم تدمرها.

ومع تزايد الاهتمام بالاتصالات اللاسلكية من الجو إلى الأرض من خلال إرسال تقارير الاستطلاع التكتيكي عن أرض المعركة، أو لتصحيح نيران المدفعية في إصابة أهدافها، ولأهمية المعلومات المتبادلة على هذه الشبكات؛ كان غالباً، ما يشوش عليها، لحرمان الجانب المعادى من الحصول على معلومات عن الأهداف المطلوب تدميرها، وكذلك حرمانه من أن يصحح نيران مدفعيته، وإصابة الأهداف بدقة.

2. الحرب الإلكترونية بين الحرب العالمية الأولى والثانية

أجرت عدة دول تجارب على قيام الطائرات بتوجيه القنابل لاسلكياً. وفي الثلاثينيات من القرن العشرين الميلادي تطورت أجهزة الإرسال بدرجة كبيرة، وأُنتجت أجهزة استقبال ذات حساسية عالية، وهوائيات دقيقة التوجيه، وهو ما أدى إلى التفكير في التداخل اللاسلكي لإفشال أعمال التوجيه.

وفي هذا الوقت، بدأت التطبيقات العملية للظواهر المكتشفة عام 1900، صدى الصوت؛ إذ كان عندما يرفع الصوت، ويسمع صدى في الإجابة، يعرف أن الصوت وصل حائطاً بعيداً، أو حاجزاً، ولا بد أنه انعكس من المكان نفسه. وهكذا، بدأ تطبيق تحديد المكان لأي جسم متحرك، مثل سفينة في البحر، إذ

يمكن من تحديد مسافة تحركها في زمن محدد، وحساب سرعتها؛ ففي البداية، يحدد مكـان الهدف المتحرك وتوقيته في موقع ما، ثم بعد فترة زمنية محددة، يعاد تحديد مكـان الهـدف وتوقيته في موقع آخر، وبحساب المسافة التي تحركهـا الهـدف، بـين المـوقعين الأول والثـاني، والزمن الذي استغرقه في قطع هذه المسافة، تحدد سرعة الهدف من المعادلة الآتية:

"السرعة = المسافة ÷ الزمن"

وقد طبق العاملون في معمل أبحاث البحرية الأمريكية ذلك، خلال تجارب اكتـشاف الـرادار عام 1922. وفي عام 1934، كان جهاز الرادار الأمريكي، قـادراً عـلى اكتـشاف الطـائرات عـلى مسافة 50 ميلاً؛ وفي هذه الفترة، كان هناك عمل مشابه، ينفذ في بريطانيا وألمانيـا. وبحلـول شهر يونيه 1935، أُنتج أول رادار نبضي للبحريـة البريطانيـة، يمكنـه كـشف الأهـداف حتـى مدى 17 ميلاً. وفي مارس 1936، أُنتج جهاز مماثـل معّـدل بمـدى كـشف 75 مـيلاً. وهكـذا، تطور تصنيع الرادارات على المسرح الأوروبي، وفي الولايات المتحدة الأمريكية.

3. الحرب الإلكترونية في الحرب العالمية الثانية

وحتى ديسمبر 1938، تمكنت الدول الأوروبية من إنتاج رادارات، ذات مـدى كـشف راداري 100 ميل عن الطائرات المعادية توفر زمن إنذار لأكثر من نصف ساعة، عن هجـوم قاذفـات القنابل المعادية، فضلاً عن إنتاج رادار بحري، يوفر مدى كشف راداري 15 ميلاً عـن القطـع البحرية المعادية.

ومنـذ أكتـوبر 1935، كلـف مـسؤول البرنـامج البريطـاني لتطـوير الـرادار بدارسـة إمكانيـة التشويش على أجهزة الكشف الراداري؛ إذ بدأت التجارب، وأمكن تحقيق نتائج إيجابيـة في عام 1938، وفي عام 1939. كما بدأت في إنجلترا دراسة إمكانيـة تـشغيل عـمال الـرادار عـلى أجهزتهم، في ظل قيام العدو بأعمال الإعاقة والتشويش، على الرادارات الإنجليزية.

ومع تزايد الانتصارات الألمانية في فرنسا وهولندا وبلجيكا، في صيف 1940، والإجلاء الـسريع للقوات البريطانية من الجزء الرئيسي مـن أوروبـا، وتزايـد إمكـان دخـول الولايـات المتحـدة الأمريكيـة الحـرب إلى جانـب الحلفـاء؛ بـدأت واشـنطن، في سريـة تامـة، بتعبئـة الهيئـات العسكرية الصناعية والعلمية وتنظيمها، لخدمة الحرب الإلكترونية.

أما الإنجاز الكبير الذي حدث بعد ذلك، هو أنه، بعد سقوط فرنـسا، هـرب العـالم "مـوريس دولورين" إلى الولايات المتحدة الأمريكية، ومعه ثلاثة من زملائه الذين كانوا يعملون في نوع جديد من أجهزة تحديد الاتجـاه ذات الـتردد العـالي للبحريـة الفرنـسية، وبـدءوا العمـل في مختبر الاتصالات اللاسلكية الفيدرالي في "أماجا نسيت" بولاية "لونـج أيلانـد" Long Island، وسرعان ما قاموا بتشغيل نموذج متطور لتحديد الاتجاه اللاسلكي يعمل عـلى الـشواطئ، ثـم طوروا جهازاً آخر للعمل بالسفن الحربية، دخل الخدمة في القوات البحرية بعد ذلك.

ومنــذ أوائــل ديــسمبر 1941، وقبــل دخــول الولايــات المتحــدة الأمريكيــة الحــرب مبــاشرة، أنتجــت رادارات متقدمــة منهــا SCR-270، ثــم SCR-271، وذلــك

بزيادة حيز تردداتها، ركبت فيما بعد، بالسفن الحربية، وحاملات الطائرات، والطرادات، مما أدى إلى التغلب على أعمال الاستطلاع والإعاقة الرادارية.

وفي الوقت نفسه، كانت الإجراءات المضادة للرادارات تسير سيراً حسناً، مثل مستقبل التحذير الراداري1 من الرادارات المعادية Radar Warning Receiver: RWR من نوع P-540، والذي تطوّر، بعد ذلك، إلى ما أطلق عليه P-587، والذي أقر في مختبر الطاقة الإشعاعية.

وهكذا، زاد التنافس بين القوات المتحاربة في المحيط الأطلسي والمحيط الهادي، مما ساعد على التطوير المستمر في معدات الحرب الإلكترونية وأعمالها، حتى وصلت إلى ما هي عليه الآن، في ظل التطور الهائل لتكنولوجيا الإلكترونيات.

وهكذا استمر الصراع الدائر للحصول على التكنولوجيا المتقدمة لإنشاء أحدث النظم الإلكترونية اللازمة للسيطرة وإدارة النيران، وللمعاونة في إدارة أعمال القتال. وكان يتبعها دائماً العمل الدائم في مراكز الأبحاث للوصول إلى أكثر المعدات الخاصة بالحرب الإلكترونية تعقيداً من وسائل للاستطلاع والإعاقة على هذه المعدات المتقدمة، التي يتم إنشاؤها. ثم يأتي دور اختبار هذه المعدات الجديدة في مجال الحرب الإلكترونية ليتم إنزالها إلى ساحة القتال، لمعرفة تأثيرها، ثم تجري أعمال التطوير مرة أخرى على ضوء ما يدرس من مزاياها وعيوبها. ظهر ذلك واضحاً في حروب ما بعد الحرب العالمية الثانية:

"كوريا ـ فيتنام ـ حرب 1967 ـ حرب 1973 ـ فوكلاند ـ سهل البقاع ـ خليج سرت ـ حرب تحرير الكويت ـ ثم حرب البلقان.

أولاً: تعريف الحرب الإلكترونية ومفهومها

للحرب الإلكترونية العديد من التعريفات العلمية، إلا أنها بالدرجة الأولى تتوقف على طبيعة الاستخدام القتالي ومفهومه المطلوب تحقيقهما في العمليات الحربية الحديثة التي تتنوع فيها النظم والوسائل الإلكترونية المتطورة لأسلحة القتال؛ تلك الأهداف المطلوب من الحرب الإلكترونية أن تتعامل معها، وتؤثر على فاعليتها، بهدف حرمانها من أداء مهامها الوظيفية بكفاءة، وبالتالي تهيئة الظروف المناسبة للقوات الصديقة من العمل في بيئة إلكترونية مناسبة تسمح بتنفيذ المهام المطلوبة بكفاءة ودقة عاليتين، وفي الزمان والمكان المناسبين.

1. تعريف الحرب الإلكترونية من ناحية تطبيقية

هي مجموعة الإجراءات الإلكترونية المتضمنة استخدام بعض النظم والوسائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم، العدو ووسائله ومعداته الإلكترونية المختلفة مع الاستخدام المتعمد للطاقة الكهرومغناطيسية في التأثير على هذه النظم والوسائل؛ لمنع العدو، أو حرمانه، أو تقليل استغلاله للمجال الكهرومغناطيسي، فضلاً عن حماية الموجات الكهرومغناطيسية الصادرة من النظم والوسائل الإلكترونية الصديقة من استطلاع العدو لها، أو التأثير عليها.

2. مفهوم الحرب الإلكترونية

انطلاقاً من هذا الفكر في تعريف الحرب الإلكترونية، فإن مفهوم الحرب الإلكترونية هو: مجموعة الإجراءات التي تنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية، وإخلال عمل هذه النظم والوسائل الإلكترونية، ومقاومة الاستطلاع الإلكتروني المعادي، وتحقيق استقرار عمل النظم الإلكترونية الصديقة تحت ظروف استخدام العدو أعمال الاستطلاع، والإعاقة الإلكترونية.

ثانياً: الأهداف الإلكترونية المعادية للحرب الإلكترونية

هي الأهداف المطلوب أن تتعامل معها الحرب الإلكترونية بأعمال الاستطلاع، والإعاقة الإلكترونية، ويمكن أن نوجز أهم هذه الأهداف فيما يلي:

1. محطات الاتصال اللاسلكي، واللاسلكي متعدد القنوات، والميكروويف.

2. أنظمة الرادار العسكرية

أ. للإنذار وتوجيه النيران.

ب. للإنذار والمراقبة الساحلية.

ج. للتوجيه لمراكز السيطرة الجوية.

د. لقيادة نيران المدفعية وتصحيحها.

هـ. لمراقبة التحركات الأرضية.

3. نظم الكشف والتوجيه الكهروبصرية "تليفزيوني، وحراري، وليزري، وبصري".

ثالثاً: مسارح الحرب الإلكترونية.

إذا كان البر، والبحر، والجو، والفضاء الخارجي، هي المسارح التقليدية للحرب، فيُعَدّ حيز المجال الكهرومغناطيسي ـ مجال انتقال الموجات الترددية بأنواعها، وأطوالها الموجية المختلفة ـ هو المسرح الحقيقي للحرب الإلكترونية؛ إذ تتنازع الأطراف المتحاربة على استغلال هذا المجال لمصلحته.

تمتد مسارح الحرب الإلكترونية من قاع المحيطات حتى الطبقات العليا للفضاء الخارجي؛ إذ يستخدم فيها مختلف النُظُم الإلكترونية: "المراقبة والكشف، والقيادة والسيطرة، والإعاقة والخداع، ورصد الأهداف، وتوجيه الأسلحة"، وجميع هذه النظم تستخدم نُظُم تحليل الإشارات Signal Processing في تحليل الموجات المنعكسة من نبضات التردد الموجي للمجال الكهرومغناطيسي.

1. مسرح العمليات البحرية

بمقدور السفن الحربية، والغواصات إصابة أهدافها خلف الأفق :Over The Horizon OTH بمعاونة نُظُم الاستطلاع الإلكتروني المتطوِّرة المحمولة جواً، وفي الفضاء الخارجي، والمتصلة بوحدات الأسطول، كما أنه بمقدور وحدات مكافحة الغواصات من طائرات، وسفن، وغواصات مسح قاع البحار والمحيطات باستخدام الأجهزة الإلكترونية "السونار"؛ للكشف عن الغواصات، والألغام البحرية المعادية في الأعماق.

2. مسرح العمليات الجوية

طائرات الإنذار المبكر، والتوجيه المحمولة جواً "أواكس"2 Airborne Warning and Control System: AWACS تبلغ فوراً عن أي اختراق معادٍ، وتوجه المقاتلات لإصابة أهدافها في الجو بدقة. كما تراقب نُظُم الاستطلاع الإلكتروني المحمولة جواً، الأوضاع والتحركات المعادية في مسرح العمليات الإستراتيجي، وتخطر غرف العمليات المركزية بها أولاً بأول، وهذا المسرح تعمل فيه الحرب الإلكترونية بكل عناصرها.

3. مسرح العمليات البرية

تتركز حالياً أعمال الحرب الإلكترونية المضادة؛ لإرباك عمل مراكز العمليات الرئيسية المعادية التي تضم نُظُم القيادة، والسيطرة، والاتصالات من طريق تعرّف ترددات الإرسال الخاصة بها، والتداخل عليها بأعمال الإعاقة اللاسلكية، الإيجابية، والخداعية، الأمر الذي قد يصعب تحقيقه في حالة استخدام هذه المراكز لنُظُم اتصالات إلكترونية متطورة، وُمؤمنة، ونظام شفرة يجري تغييره باستمرار، فيصعب التداخل عليها، فضلاً عن استخدام مواقع تبادلية يجري التنقل بينها، وفي هذه الحالة يكون من المفضل التعامل معها بأعمال التدمير.

رابعاً: أهمية الحرب الإلكترونية

تحتل أعمال الحرب الإلكترونيـة، في الوقـت الحـاضر، مكانـاً بـارزاً بـين الأنـشطة العـسكرية الأخرى. ويولي كافة الأطراف، من الـشرق أو الغـرب، الكثـير مـن الاهـتمام لتطـوير وسـائلها وأساليب استخدامها بعد أن أثبتت خبرات الحـروب المحـدودة التـي تلـت الحـرب العالميـة الثانية أهميتها، سواء في الدفاع أو الهجوم.

وقد أحدث اسـتخدام معـدات الحـرب الإلكترونيـة في الحـروب الحديثـة تطـوراً هـائلاً في مجالات هذه الحروب ومراحلها، وأصبح الحسم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الحديث منها، وبقدر ما يمتلكه كل طـرف مـن الأطـراف المتـصارعة، بعـد أن كانت تحسم لمصلحة الطرف الذي يمتلـك التفـوق العـددي، أو النـوعي، أو يمتلـك الأسـلحة البعيدة المدى، والدليل على ذلك أن معـدات الحـرب الإلكترونيـة المـستخدمة في الطـائرات المقاتلة يقترب ثمنها من نصف قيمة الطائرة.

في مجال أعمال الحرب الإلكترونية الدفاعية Defensive Measures. EW يوفر الاستطلاع الإلكتروني رصيداً من المعلومات عن الأوضاع والتحركات في مسرح العمليات المنتظر، وكذلك خصائص معدات العدو الإلكترونية، لاتخاذ الإجراءات الإلكترونيـة المـضادة؛ لمواجهتهـا. كـما يتيح التعرف على نُظُم المواصـلات، وشـبكات المعلومـات التـي تـربط مراكـز قيـادة العـدو بتشكيلاته ووحداته، مما يسمح بالتـداخل عليهـا بالـشوشرة والإعاقـة لإرباكهـا، وفي الوقـت نفسه، اتخاذ الإجراءات الكفيلة بتحقيق أمن السيطرة على المواصلات الصديقة، وعدم تمكين العدو من التداخل عليها.

في مجال أعمال الحرب الإلكترونية الهجومية Offensive Measures. EW يركز في بداية العمليات على تدمير مراكز الحرب الإلكترونية المعادية؛ بما يتيح حرية عمل الأسلحة الصديقة الموجهة، وتحقيق الدقة في إصابتها لأهدافها. كما تستخدم نُظُم المعلومات الميدانية المتطورة التي تضم المستشعرات السلبية، والحاسبات الآلية، ونظم التحكم الآلي، لتحديد الأهداف المعادية بدقة، واستخدام نُظُم الذخيرة الدقيقة التوجيه لتدميرها. ويُعَدّ إبطال فاعلية مواصلات مراكز القيادة والسيطرة الآلية المعادية عن طريق الإجراءات الإلكترونية المضادة الصديقة، في مقدمة أولويات الحرب الإلكترونية؛ لذلك يجري التخطيط لذلك مسبقاً قبل بدء العمليات، فإخماد أو إبطال عمل مراكز القيادة والسيطرة المعادية مبكراً يعني النهاية للحرب، وهو ما أثبتته عمليات الحرب الإلكترونية التمهيدية الناجحة للطائرات الحليفة في عملية "عاصفة الصحراء" في حرب الخليج الثانية.

خامساً: أهمية تكامل أنظمة الحرب الإلكترونية

أضاف تخصيص طائرات خاصة لأعمال الحرب الإلكترونية بعداً جديداً تمثل في استخدام أنظمة متكاملة للحرب الإلكترونية INEWS Integrated Electronic Warfare System، اشتملت على جانب من عالم الحرب الكهروبصرية؛ إذ يستخدم الليزر، والأشعة تحت الحمراء، والتليفزيونية في النظام "ترام" Target Recognition Attack Multi-Sensors TRAM، أي نظام تمييز الأهداف متعدد المستشعرات؛ لأغراض الهجوم.

يستخدم النظام ترام المحمول جواً أجهزة للرؤية الأمامية بالأشعة تحت الحمراء Forward Looking Infrared: FLIR؛ لتظهر الصورة على شاشة تليفزيونية بكابينة الطيار في تكامل مع أنظمة تحديد المدى بأشعة الليزر من طريق إضاءة الهدف ليزرياً، كما يوجد في مقدمة الصاروخ آلة تصوير تليفزيونية تعمل في مستوى الضوء المنخفض Low Light Level TV: LLLTV ترسل صوراً واضحة إلى الطائرة، لتستخدم في أغراض التوجيه التليفزيوني، وذلك مع وجود جهاز تسجيل خاص، تسجل عليه صور الأهداف بالفيديو لاستعادتها فورياً؛ لأغراض المقارنة والتطابق مع الأهداف الحقيقية المطلوب تدميرها، وكذلك لتقدير كفاءة الضرب، وهو ما يسمى "نظام دمج المعلومات" Data Fusion.

هكذا، يسمح النظام "ترام" الموجود في الطائرة EA-6B بتمييز الأهداف التي تظهر بالرادار مع إمكانية توجيه ضربة بالأسلحة الموجهة ـ بأشعة الليزر، بالتليفزيون، بالأشعة تحت الحمراء ـ بدقة متناهية، في الوقت الذي تنفذ فيه الطائرة مناورات عالية فوق الهدف، ويؤدي استخدام الأسلحة الذكية Smart Weapons إلى الإصابة الدقيقة من الطلقة الأولى؛ إذ إن الطائرة لا تستطيع، في ظروف الدفاع الجوي بأنظمته الحديثة، أن تتمهل في منطقة الهدف، أو أن تعاود الكرة مرة أخرى؛ إذ يغدو الثمن غالياً. ولا شك في أن حمل الطائرة للأسلحة الذكية باستخدام أسلوب "أطلق وانسَ"Fire and Forget يحميها ويساعدها على تفادي الأسلحة المعادية. وهكذا، يساعد النظام "ترام" على

تحـسين الأداء، وزيـادة القـدرة عـلى العمـل بكفـاءة في ظـل وجـود التهديـدات الكثيفـة والمعقدة.

من أشكال الدعم بـالحرب الإلكترونيـة في الحـروب الحديثـة، أنـه يمكـن لطـائرات القتـال المجهّزة بمعدات الحـرب الإلكترونيـة، أن تعمـل مـصاحبة للطـائرات المقاتلـة القاذفـة أثنـاء قيامهـا بـالاختراق العميـق؛ لـستر تقـدمها بـأعمال الإعاقـة الإلكترونيـة المـصاحبة Escort Jamming ضـد رادارات الـدفاع الجـوي المعـادي، وهـي مـا تعـرف بالمـساندة الإلكترونيـة القريبة، أو مـن خـلال المـساندة بالإعاقـة الإلكترونيـة البعيـدة باسـتخدام طـائرات الحـرب الإلكترونية من مظلات بعيدة عن مرمى الدفاع الجوي المعـادى، يطلـق عليهـا Stand-Off Jamming، ويتوقف ذلك على متطلبـات تحقيـق المهمـة، ففـي الوقـت الـذي تفـضل فيـه القوات البحرية النوع الثاني Stand-Off Jamming فإن القوات الجوية تفضل النـوع الأول من أعمال المساندة الإلكترونية Escort Jamming، وهي مهمة الحراسة، والمرافقـة بـأعمال الدعم الإلكتروني.

سادساً: أقسام الحرب الإلكترونية

تعتمد تكتيكات الحرب الإلكترونية على اسـتخدام وسـائل ونظـم إلكترونيـة تتـيح اسـتغلال الحيز الكهرومغناطيسي لصالح طرف وحرمان الطـرف الآخـر أو خداعـه عـن اسـتغلال هـذا الحيز، وهو ما أدى إلى تقسيم الحرب الإلكترونية إلى الأقسام التالية:

1. الإجراءات الإلكترونية المضادة Electronic Counter Measures ECM:

وهي تعني تنفيذ الأعمال الآتية:

أ. أعمال الإعاقة الإلكترونية الإيجابية والسلبية.

ب. أعمال التدمير للنظم، والوسائل، والمعدات الإلكترونية المعادية.

2. أعمال الاستطلاع الإلكتروني Electronic Reconnaissance

وهو ما يطلق عليه اسم "المساندة الإلكترونية" Electronic Support Measures ESM.

ويُطلق عليه الاستطلاع الإلكتروني للنظم الإلكترونية المعادية أو أعمال المساندة الإلكترونية، إذ يؤدي الاستطلاع الإلكتروني دوراً إستراتيجياً في تحديد تكتيكات العدو، وإمكاناته، وأهدافه، وينفذ خلال السلم والحرب، وقبل العمليات وأثناءها من خلال النظم والمعدات الإلكترونية ذات التقنية العالية التي تزود بها الطائرات، والسفن، والأقمار الصناعية. ويكشف الاستطلاع الإلكتروني، على المستوى التكتيكي، نوع دفاعات العدو، وإمكاناته، وقدراته من الأسلحة، ومعدات القتال، فضلاً عن تقويم النظم، والوسائل، والمعدات الإلكترونية؛ بما يساعد على تطوير معدات الحرب الإلكترونية الصديقة وإعادة برمجتها؛ لمواجهة النشاط الإلكتروني المعادي.

لا شك أن الاستطلاع الإلكتروني، يُعد حالياً، من أهم مصادر الحصول على المعلومات وأحدثها في معظم جيوش العالم، وقد تطور بـشكل كبـير جـداً؛ نتيجـة للتطـور الهائـل في تكنولوجيـا الإلكترونيات، واعتماده على الخـصائص الفنيـة للموجـات الكهرومغناطيـسية، التـي يـسهل متابعتهـا، فـضلاً عـن أن المعـدّات الإلكترونيـة أصـبحت إحـدى الـسمات المميـزة للحـروب الحديثة، كما أن الاستطلاع الإلكـتروني يُعـد كـذلك إحـدى سـمات هـذه الحـروب في مجـال الحصول على المعلومات.

3. الأعمال الإلكترونية المضادة لإجراءات الحرب الإلكترونية المعادية

Electronic Counter Counter Measures ECCM

تعني التأمين الإلكتروني للنظم، والوسائل الإلكترونية الصديقة من أعمال الحرب الإلكترونيـة المعادية، وتشتمل على ما يلي:

أ. إجراءات مقاومة الاستطلاع الإلكتروني المعادي.

ب. وقاية النظم، والوسائل، والمعدات الإلكترونية الصديقة من الإعاقة الإلكترونية المعادية.

ج. وقاية النظم، والوسـائل، والمعـدات الإلكترونيـة الـصديقة مـن وسـائل التـدمير المعاديـة الموجهة إلكترونياً، أو المضادة لمصادر الإشعاع الكهرومغناطيسي.

د. المراقبة الإلكترونية للإشعاعات الكهرومغناطيسية الصديقة، وهي تعني الآتي:

(1) منع التعارض الكهرومغناطيسي للنظم، والوسائل الإلكترونية الصديقة من التداخل الصديق الذي يحدث نتيجة لسببين رئيسيين:

(أ) أن عددا كبيراً من النظم والوسائل الإلكترونية الصديقة يعمل في مساحات محددة في وقت واحد، وبكثافة عالية.

(ب) عدم التزام بعض القوات، بتعليمات التأمين الإلكتروني في تشغيل النظم والوسائل الإلكترونية، مثل استخدام إحدى الوحدات ترددات لاسلكية مخصصة لوحدة أخرى؛ فيحدث التداخل الكهرومغناطيسي.

(2) أدى ذلك إلى إضافة مهمة جديدة للقادة والقيادات على مختلف المستويات، هي:

(أ) التنظيم الفني والتكتيكي للنظم والوسائل الإلكترونية، لضمان منع هذا التعارض الكهرومغناطيسي أثناء تشغيل الوسائل الإلكترونية الصديقة.

(ب) تشكيل عناصر مراقبة إلكترونية مهمتها التأكد الدائم من التزام القوات بتعليمات التشغيل الفني والتكتيكي من خلال استخدام معدات إلكترونية؛ لقياس النشاط الإشعاعي الصديق ومراقبته، في منطقة عمل القوات، إضافة إلى اكتشاف أي إشعاع أجنبي يبث داخل المنطقة.

الأعمال الإلكترونية المضادة ECM

الأعمال أو الإجراءات الإلكترونية المضادة ECM Electronic Counter Measures تعني اكتشاف النظم الإلكترونية؛ لسيطرة العدو على قواته،

وأسلحته، ومعداته؛ لتحديد حجم، قواته وأوضاعها، ووسائل إنتاج النيران، بهدف شلّه، أو إفقاده سيطرته على قواته، وأسلحته، بأعمال الإعاقة الإلكترونية، أو بأعمال التدمير لهذه النظم، وذلك لتقليل فاعلية الاستخدام القتالي لقواته، وتقليل كفاءة أسلحته التدميرية في إصابة أهدافها من خلال الأعمال أو الإجراءات الإلكترونية الآتية:

- الإعاقة الإلكترونية للنظم الإلكترونية اللاسلكية/ الرادارية/ والكهروبصرية/ والصوتية/ والحاسبات الآلية المعادية.

- تدمير النظم الإلكترونية المعادية باستخدام النبضة الكهرومغناطيسية EMP، أو أسلحة الطاقة الموجهة DEW.

أولاً: مفهوم الإعاقة الإلكترونية

تُعد إعاقة نظم العدو ووسائله الإلكترونية، أحد الإجراءات الإلكترونية المضادة Electronic Counter-Measures: ECM المهمة التي تقوم على فكرة إعاقة تشغيل النظم، والوسائل الإلكترونية المعادية بأنواعها المختلفة من خلال التأثير على كفاءتها في أداء مهامها الوظيفية بأساليب الإعاقة الإلكترونية الآتية:

- الإعاقة الإلكترونية الإيجابية: وتعتمد في إعاقة تشغيل النظم والوسائل الإلكترونية المعادية المختلفة (لاسلكية، رادارية، كهروبصرية... إلخ) على خاصية التقاط أجهزة الاستقبال للإشارات المرغوبة، والإشارات الأخرى غير المرغوبة التي تكون على التردد نفسه.

- الإعاقة الإلكترونية السلبية: تعتمد الإعاقة السلبية في إعاقة تشغيل النظم والوسائل الإلكترونية المعادية المختلفة على خاصية انعكاس الإشعاعات الكهرومغناطيسية؛ سواء من الأجسام المرغوبة، أو غير المرغوبة التي تصطدم بها لترتد مرة أخرى إلى أجهزة استقبال هذه النظم والوسائل.

1. الإعاقة الإلكترونية الإيجابية

أ. تعريف الإعاقة الإلكترونية الإيجابية

هي عملية توجيه حزمة من الأشعة الكهرومغناطيسية المتعمدة إلى مستقبلات النظم والوسائل الإلكترونية المعادية؛ للتأثير على أدائها بتعميتها، أو خداعها بهدف شل، عملها وإرباكه.

وببساطة شديدة، يمكن القول، بأن الإعاقة الإلكترونية الإيجابية هي عملية إرسال إشعاع متعمد لموجات كهرومغناطيسية يتم إصداره من جهاز ما ـ لاسلكي، راداري،... الخ ـ وتوجيهه في اتجاه جهاز استقبال معين؛ بغرض فرض هذا الشعاع دون سواه على هذا المستقبل.

ب. العوامل المؤثرة على مدى فاعلية الإعاقة الإلكترونية الإيجابية

(1) العلاقة بين قدرة محطة الإعاقة، وقدرة جهاز الإرسال المعادي.

(2) العلاقة بين مسافة محطة الإعاقة، ومسافة جهاز الإرسال المعادي، بالنسبة لجهاز الاستقبال المعادي.

(3) العلاقة بين قوة الإشارة المستقبلة من محطة الإعاقة، وقوة الإشارة المستقبلة من جهاز الإرسال المعادي عند نقطة التقاط هوائي جهاز الاستقبال المعادي.

(4) نوع الهوائيات المستخدمة في كل من محطة الإعاقة، وجهاز الاستقبال المعادي ـ استخدام هوائيات موجهة/ غير موجهة.

وهذه العوامل تعني أنه كلما زادت قدرة الإعاقة بالنسبة لقدرة إشارة جهاز الإرسال المعادي الواصلة لجهاز الاستقبال، ازداد تشويه هذه الإشارة، وعندما تصل قدرة الإعاقة إلى حد معين، تضيع الإشارة نهائياً، ولا يمكن تمييزها بجهاز الاستقبال، والإعاقة التي يمكنها إخماد الإشارات بأقل نسبة قدرة، تُسمى "بالإعاقة القصوى".

ج. مراحل الإعاقة الإلكترونية الإيجابية

(1) مرحلة البحث: وفيها تستخدم محطة بحث إلكتروني تكون مهمتها مسح الحيز الكهرومغناطيسي المتوقع أن تعمل فيه الأهداف الإلكترونية المعادية؛ لالتقاط الإشعاع الكهرومغناطيسي الصادر من هذه الأهداف، ثم تقدر أهميتها، وتبعيتها، وترسل بياناتها إلى عناصر التحديد؛ لتعيين أماكنها.

(2) مرحلة تحديد موقع الهدف: وفيها تستخدم محطات تحديد الاتجاه لرصد زوايا الهدف وتبلغها إلى مركز التحديد؛ لتحديد مكان الهدف على الخريطة، وتبليغ إحداثياته إلى جهات البحث والتوجيه الإلكتروني.

(3) مرحلة توجيه الإعاقة: وفيها توجه محطة البحث والتوجيه محطات الإعاقة الإلكترونية على الهدف المراد إعاقته، بإعطائها البيانات الفنية الدقيقة للهدف، وكذلك اتجاهه، ومكانه من موقع محطة الإعاقة، والتأكد من تمام تمييزها لهذا الهدف، والقبض عليه.

(4) مرحلة تنفيذ الإعاقة: وتبدأ بعد تمييز الهدف، طبقاً لبيانات محطة البحث والتوجيه، تنفذ محطة الإعاقة أعمال الإعاقة ضد الهدف.

(5) مرحلة مراقبة مفعول الإعاقة: وفيها تراقب محطة البحث، والتوجيه مدى تأثير الإعاقة على الهدف المعادي، واكتشاف أي تغيير في بياناته الفنية (تردد، نداءات،... الخ)، للهروب من الإعاقة، وبالتالي تبلغ هذه البيانات أولاً بأول لمحطات الإعاقة؛ لإعادة دورة الاشتباك بالإعاقة، طبقاً للبيانات الجديدة.

2. الإعاقة الإلكترونية السلبية

أ. تعريف الإعاقة الإلكترونية السلبية

هي عملية انعكاس متعمد للإشعاع الكهرومغناطيسي الصادر من أجهزة إرسال النظم والوسائل الإلكترونية المعادية، وخاصة الرادارية، نتيجة لإجبارها على الاصطدام بأجسام معينة دون سواها، فيرتد هذا الشعاع مرة أخرى نحو مستقبلات هذه النظم، والوسائل المعادية، مسبباً إرباكها، وتقليل كفاءتها، في تنفيذ مهامها.

ب. مزايا أعمال الإعاقة الإلكترونية السلبية

(1) يمكن تنفيذها دون الحاجة إلى المعرفة الدقيقة لأماكن وسائل العدو الإلكترونية.

(2) يجري عملها مع بدء قيام النظم والوسائل الإلكترونية المعادية في العمل.

(3) تحتاج أعمال الإعاقة الإلكترونية فقط إلى معرفة الاتجاه.

ثانياً: أعمال الإعاقة اللاسلكية والرّادارية:

1. أعمال الإعاقة اللاسلكية

تستخدم الإعاقة اللاسلكية في الإخلال بمواصلات العدو اللاسلكية، واللاسلكية متعددة القنوات، وتنقسم إلى:

أ. الإعاقة اللاسلكية الإيجابية

يُقصد بالإعاقة اللاسلكية الإيجابية، ذلك الإشعاع الكهرومغناطيسي المتعمد الذي يوجه ضد مستقبلات الأجهزة والمحطات اللاسلكية المعادية، والتي بالتأثير عليها، تُفقد العدو سيطرته على قواته.

ولضمان تنفيذ إعاقة لاسلكية مؤثرة، لا بد أن تتطابق الإعاقة على الإشارة اللاسلكية المستقبلة.

وتنقسم الإعاقة اللاسلكية طبقاً للتطابق بين الإشارة والإعاقة إلى:

(1) الإعاقة الموضوعية Spot Jamming: هـي التـداخل اللاسـلكي الـذي يهـدف إلى إخـماد مواصـلة لاسـلكية واحـدة، ولا يزيـد حيـز تـرددات الإعاقـة الموضـوعية عـن عـرض النطـاق الترددي، للإشارة المراد إعاقتها.

(2) الإعاقة بالغلالة Barrage Jamming: هي الإشعاع اللاسلكي في حيز ترددات واسـع، قـد تعمل فيه عدة محطات لاسلكية معادية يراد إعاقتها.

(3) الإعاقـة الزاحفـة نقطـة متحركـة في حيـز Sweep Jamming: وتكـون بإشـعاع طاقـه كهرومغناطيسية مركزة في حيز تردد ضيق في زمن معين، ثم الانتقال إلى تردد آخر مجاور.

وتنقسم الإعاقة اللاسلكية الإيجابية، طبقاً لطريقة التحكم ـ توجيه الإشعاع ـ إلى:

(1) إعاقة موجهة: وتكون بتركيز الطاقة المشعة في اتجاه الهدف المراد إعاقته.

(2) إعاقة غير موجهة: وتكون بإنتاج الطاقة المشعة في جميع الاتجاهات بالتساوي.

وتنقسم الإعاقة اللاسلكية الإيجابية طبقاً لدرجة التأثير إلى:

(1) إعاقة كاملة "إخماد": تـشوه فيهـا 50% مـن المعلومـات المـستقبلة، ويـصبح الاسـتقبال مستحيلاً، حيث تقلل كفاءة الاستقبال، بدرجة تصل إلى 90% من الإشارة الأصلية.

(2) إعاقة قوية: تسبب فقد 30% من المعلومات.

(3) إعاقة ضعيفة: تسبب فقد 15% من المعلومات.

ب. الإعاقة اللاسلكية الإيجابية الخداعية

وتجري باستخدام إشارات لاسلكية مدبرة تحمل معلومات خداعية.

2. أعمال الإعاقة الرادارية

تستخدم نظم الإعاقة الرادارية في شل، وسائل السيطرة الرادارية المعادية وإرباكها وخداعها، سواء الأرضية، أو المحمولة بحراً/ جواً، والمستخدمة في أعـمال الكـشف، والتتبـع، والتوجيـه، والتحكم لأسلحة القتال الحديثـة، وخاصـة أثنـاء العمليـات الليليـة؛ لتقليـل نـسب إصـابتها لأهدافها.

وتنقسم نظم الإعاقة الرادارية، طبقاً لنوع وسائل الإعاقة المستخدمة، إلى:

أ. نظم الإعاقة الإيجابية

تصمم الإعاقة الرادارية الإيجابية؛ لتكون قادرة عـلى التعامـل مـع معظـم أنـواع الـرادارات المعادية الحديثة، بما يمكنها من استطلاع هذه الرادارات وتمييزها، مع الـسرعة في رد الفعـل، طبقاً لأسبقيات التهديد.

(1) متطلبات الإعاقة الرادارية الإيجابية

(أ) يجب أن تشتمل على عناصر استطلاع راداري.

(ب) توجيه إعاقـة مـؤثرة مطابقـة لمواصـفات الأهـداف المعاديـة مـع اسـتمرار تتبـع تلـك الأهداف.

(ج) توفير اتصالات مباشرة للتعاون مع نظم الإعاقة الأخرى؛ لإمكان تبـادل المعلومـات عـن الأهداف المعادية.

(د) إمكانية المناورة بالإعاقة من هدف مُعادٍ لآخر.

(2) الشروط الواجب توافرها في مرسل الإعاقة الرادارية الإيجابية

(أ) يجب أن يتواءم التردد المستخدم في مرسل الإعاقة مع تردد في المستقبل ـ الرادار المعادي ـ المراد إعاقته.

(ب) التداخل بصفة مستمرة على مستقبل الرادار المعادي.

(ج) يجب الوضع في الحسبان، عند تصميم مرسل الإعاقـة، أن هنـاك عوامـل خارجيـة تـؤثر عـلى مفعـول الإعاقـة، مثـل اضـمحلال الإشـارة في الغـلاف الجـوي، وتـشتيتها مـن طبقـة التربوسفير، وظاهرة الحرارة والطقس، هذا بالإضـافة إلى بعـض العوامـل الأخـرى الواضـحة، مثل:

- ما يعرف باسم Burn Through Range، وهو أقصى مـدى كـشف راداري تحـت تـأثير الإعاقة الضوضائية المعادية.
- صفات الرادار المعادي.

ب. طرق الإعاقة الرادارية الإيجابية وأنواعها:

تنقسم طرق الإعاقة الإيجابية إلى ثلاثة أنواع:

(1) الإعاقة الضوضائية: Noise Jamming

وهي تعني الإعاقة بالشوشرة، التي تنتج بتعديل التردد التكراري Repetition Frequency: RF بالشوشرة ـ تغييراً عشوائياً في القيمة، وترسل هذه الشوشرة على تـردد الـرادار المعـادي. وتبنى فكرة عمل الرادار لتمييز الأهداف على إرسال نبضة تصطدم بالهدف، ثم ترتـد هـذه النبضة من الهدف، ويستقبلها مستقبل الرادار، ولكنها تكون ضعيفة جداً؛ لهذا فإن مستقبل الرادار يصمم بحيث يكون ذا حساسية كبيرة؛ ليمكنه استقبال هذه النبضة الضعيفة، وتمييز الهدف. وهذه الحساسية لمستقبل الرادار المعادي، في الواقع، هي التي تجعل إشارة الإعاقـة بالشوشرة لها قدرة كبيرة على اقتحـام هـذا المـستقبل؛ إذ إن إشـارة الإعاقـة تكـون كبـيرة في قيمتها عن إشارة الرادار المرتدة من الهدف، وهذا النوع من الإعاقة هو مـا يعـرف بالإعاقـة الضوضائية، والذي ينفذ بالطرق الآتية:

(أ) الإعاقة الغلالية Barrage Jamming

وهي تعني تنفيذ الإعاقة على حيز عريض من الترددات، في وقت واحد.

(ب) الإعاقة الموضعية المركزة Spot Jamming

وهي تعني تنفيذ الإعاقة على حيز ضـيق نـسبيا، يـساوي تقريبـاً حيـز تـردد إشـارة الـرادار المعادي المراد إعاقته.

(ج) الإعاقة الزاحفة Sweep Jamming

وهي تعني تركيز قدرة عالية لإشارة الإعاقة خلال حيز واسع من الترددات، ويتم تنفيذ ذلك بإشعاع طاقة كهرومغناطيسية مركزة في حيز ترددي ضيق.

(د) الإعاقة الزاحفة القافلة Sweep Lock Jamming

وتعني هذه الطريقة إمكانية قيام جهاز الإعاقة بإرسال إشارة إعاقة ضيقة جداً، تولف على حيز ترددي واسع، مع قفل هذه الإشارة "الإعاقة" داخل حيز التردد الخاص بجهاز الاستقبال لرادار المعادي؛ بمعنى أن مرسل جهاز الإعاقة يزحف داخل حيز تردد جهاز الاستقبال للرادار المعادي، وفي الوقت نفسه فإن مرسل جهاز الإعاقة هو جهاز إعاقة مركزة على تردد معين.

(هـ) الإعاقة بالنبضة المغطاة Cover Pulse Jamming

تعرف أجهزة الإعاقة التي تعمل بنظام النبضة المغطاة بأجهزة الشوشرة الضيقة، وهذا النوع يستخدم بكثرة، بصفته إحدى وسائل الإعاقة الإيجابية في الإعاقة على الرادارات المعادية القريبة.

(و) الإعاقة بالفص الجانبي Side Lobe Jamming

هذا النوع يستخدم في إعاقة رادارات التتبع بإدخال طاقة كبيرة من طاقة جهاز الإعاقة داخل بوابة تتبع زاوية واحدة.

أما في حالة استخدام هذا النوع في إعاقة رادارات البحث، فتؤدي الإعاقة إلى تعمية قطاع كبير على شاشة الرادار المعادي.

(2) الإعاقة الخداعية النبضية Pulse Jamming

هي أجهزة تستقبل نبضة الرادار المعادي، ثم تعيد إرسالها إليه مرة أخرى، لتظهر على شاشته هدفاً خداعياً كاذباً.

(3) الإعاقة المعدلة "الضوضائية/ النبضية" Modulated Jamming

وهذا النوع من الإعاقة، هو مزيج من الإعاقة الضوضائية "الإعاقة بالشوشرة"، والإعاقة النبضية (الخداعية). ويستخدم ضد رادارات التتبع المعادية، وضد رادارات البحث المخروطي.

ج. نظم الإعاقة السلبية Passive Jamming

وسائل الإعاقة السلبية: هي رقائق معدنية، وعواكس ركنية، وشباك معدنية، ومواد ماصة للإشعاع، تُعّد من الأساليب الفعالة، لإرباك، النظم الرادارية الحديثة، وخداعها.

(1) الرقائق المعدنية CHAFFS

تستخدم الرقائق المعدنية في إنتاج إعاقة سلبية مُنَشَّنة Spot Chaff، أو إعاقة سلبية غلالية Barrage Chaff، طبقاً لأطوال الموجة المستخدمة في الرقائق المعدنية، فإذا كانت أطوال هذه الموجة في العبوة الواحدة متساوية، تعرف بالإعاقة السلبية المنشنة Spot Passive Jamming، أما إذا كانت الأطوال غير متساوية، فتعرف بالإعاقة السلبية الغلالية Barrage Passive Jamming، أي أنه، يمكن استخدام عبوة واحدة، بداخلها عدة خراطيش، من الرقائق المعدنية المختلفة الأطوال؛ لتغطي أكثر من نطاق ترددي.

وتتوقف فاعلية الإعاقة باستخدام الرقائق المعدنية على: طبيعة الهدف المراد حمايته، ومساحة المقطع الراداري للهدف المطلوب حمايته Radar Cross

Section RCS ، والتردد الحامل للرادار Frequency Of Carrier FC المعادي المطلوب خداعه، وكثافة الرقائق المعدنية المستخدمة.

(2) العواكس الركنية Corner Reflectors

هي مجموعة من الأسطح المتماثلة، أو المربعة، أو الدائرية المتعامدة، وتأخذ أشكالاً مختلفة، منها الهرمية، والمخروطية الشكل؛ لتعطي التأثير المتساوي من جميع الاتجاهات.

وتُعد العواكس الركنية إحدى وسائل الإعاقة السلبية الفعالة، لخداع النظم الرادارية المعادية، وخاصة المحمولة جواً، لاستخدامها في التمثيل الخداعي، لمواقع الأهداف الأرضية، مع إمكانية استخدامها في تشويه المقطع الراداري للأهداف الحيوية.

وتستخدم العواكس الركنية؛ لتمثيل مواقع وأهداف حيوية، ويجب توفر معلومات عن الرادار المعادي، ومعلومات عن الهدف الحيوي؛ لتحديد مواصفات العواكس الركنية المطلوبة.

واستخدام العواكس الركنية يحقق على شاشة الرادار المعادي ما يلي:

(أ) موازنة الإضاءة بين الأجزاء المعتمة والأجزاء المضيئة على الشاشة؛ لإخفاء الهدف، فيما يعرف بالإخفاء الراداري.

(ب) إيجاد أهداف هيكلية في شكل نقط مضيئة كاذبة على شاشة جهاز الرادار المعادي، مع النقطة المضيئة للهدف الحقيقي، فيما يعرف بالخداع الراداري السلبي.

(ج) تغيير معالم الأهداف والأغراض الحيوية، بمعنى تشويه المقطع الراداري للهدف/ الغرض الحيوي، فيما يعرف بالتمويه الراداري.

(3) الستائر المعدنية

وهي ستائر من المعدن ذات تصميم خاص، ويتم تثبيتها على الأرض على مسافات محددة محسوبة، وذلك بهدف إخفاء الأهداف والتحركات الأرضية من أعمال الكشف الراداري المعادي.

(4) المواد الماصة للأشعة الرادارية

أدى التطور التكنولوجي الهائل، في مجال البتروكيماويات إلى التوصل لمواد تقلل كثيراً من المقطع الراداري للأهداف؛ إذ تمثل المواد الماصة للأشعة الرادارية أحدث ما على الساحة لأغراض الإعاقة السلبية، بغرض الإخفاء الراداري للأهداف، فبتغطية الهدف بطبقة من هذه المواد، يمكن امتصاص شبه تام للطاقة الكهرومغناطيسية، فلا يرتد منها سوى جزء بسيط.

وأمكن كذلك إنتاج بعض المواد الماصة للموجات الصوتية "السوناريه"؛ لتغطية جسم الغواصات، بصورة تؤثر كثيراً على استخدام أنظمة الكشف الصوتي "السونار" المعادية.

3. أعمال الإعاقة الكهروبصرية

نتيجة للتطور التكنولوجي السريع والهائل الذي أدى إلى استخدام النظم والوسائل الحرارية، والليزرية، والتليفزيونية في العديد من التطبيقات العسكرية باستخدامها في مجال الكشف، والتتبع، والتحكم، والقصف لأسلحة القتال الحديثة، برية/ وبحرية/ وجوية/ ودفاع جوي، وخاصة في العمليات الليلية؛ الأمر الذي استوجب ضرورة البحث عن وسائل وأساليب غير تقليدية ذات فاعلية؛ لتنفيذ أعمال الإعاقة الإلكترونية ضد هذه النظم والوسائل، التي من المنتظر استخدامها في العمليات المقبلة من خلال نظام متكامل لأعمال الإعاقة الحرارية، والليزرية، والتليفزيونية.

4. أعمال الإعاقة الحرارية

من الضروري الاهتمام بالأعمال المضادة للأشعة تحت الحمراء، وذلك لتقليل مفعول نظم المستشعرات والأسلحة، والصواريخ الموجهة بالأشعة تحت الحمراء؛ إذ تعتمد معظم الأعمال المضادة للأشعة تحت الحمراء على الآتي:

أ. تقليل الإشعاع الحراري المنبعث من الهدف ذاتياً، أو من انعكاس الشمس عليه باستخدام وسائل التبريد، لمصادر الإشعاع Shielding، أو باستخدام مولدات الدخان الحراري؛ لتشتيت جزء كبير من الإشعاع الحراري، أو باستخدام الطلاءات الماصة للحرارة.

ب. إيجاد مصدر إشعاع حراري آخر بجانب الهدف باستخدام المشاعل الحرارية "مستودعات"، كرات نيران، وأهداف مقطورة، والمرماش Blinker، والعواكس الحرارية.

أ. المشاعل الحرارية

عملية استخدام المشاعل الحرارية، ليست كما يتصورها البعض، بأنها عملية إطلاق المشاعل الحرارية من القواذف بطريقة عشوائية، ولكن يراعى فيها قياس البصمة الحرارية.

ب. خواص المشاعل الحرارية

(1) وقود من بودرة الماغنسيوم، أو الألومنيوم، أو جسم يسمح للمشعل بالبقاء في الجو، أو بالهبوط البطيء.

(2) تعطي احتراقاً متجانساً ومنتظماً طوال فترة الإشعال.

ولضمان نجاح استخدام المشاعل الحرارية، يجب أن يوضع في الحسبان الآتي:

(1) الحيز الترددي للأشعة تحت الحمراء.

(2) مستوى طاقة حرارية مناسبة خلال زمن الاشتعال.

(3) تأخير زمن الاشتعال.

5. أعمال الإعاقة التليفزيونية

تستخدم مولدات وعبوات الدخان؛ لإنتاج سحابات الدخان.

6. أعمال الإعاقة الليزرية

تنفذ أعمال الإعاقة الليزرية، ويمكن استخدام الدخان ـ نوعية خاصة ـ لتنفيذ أعمال الإخفاء الليزري، حيث إن حبيبات الدخان يمكنها تشتيت أشعة الليزر وامتصاصها.

7. أعمال الإعاقة للنظم الإلكترونية الأخرى

أ. أعمال الإعاقة الصوتية Sonar Jamming

تشتمل أعمال الإعاقة الصوتية على الأقسام التالية:

(1) أجهزة الإعاقة الصوتية ذاتية الحركة/ مقطورة

هي وسائل لتنفيذ الإجراءات الإيجابية المضادة لأجهزة الكشف الصوتي السلبي "السونار".

(2) مولدات الإعاقة الصوتية ذاتية الحركة

هي وسائل إجراءات الإخفاء/ الخداع المضادة لأجهزة الكشف الصوتي السلبي، وتستخدم في تنفيذ أعمال الإعاقة الصوتية، وتُعد هذه المعدات ذات فاعلية كبيرة؛ إذ يؤدي الاستخدام السليم لها إلى إضعاف النظم والوسائل الصوتية المعادية المستخدمة في أعمال الكشف، والتوجيه، والتحكم، وخاصة لأسلحة القتال البحري ضد الغواصات.

ب. أعمال الإعاقة الإلكترونية للحاسبات الآلية

أثبتت الأحداث خلال السنوات القليلة الماضية، بما لا يدع مجالاً للشك، أن فيروس الحاسب الآلي قد أصبح حقيقة واقعة ذات تأثير بالغ الخطورة؛ سواء على أنظمة الحاسبات، أو شبكات الحاسبات؛ إذ إن الأنظمة العسكرية الحديثة تعتمد اعتماداً كبيراً في أدائها لمهامها على النظم الإلكترونية القائمة، أساساً، على نظم وشبكات الحاسبات الآلية؛ لذلك أصبحت هذه النظم العسكرية أكثر تعرضاً للاختراق والهجوم عن مثيلتها من الأنظمة العسكرية التقليدية.

(1) فيروس الحاسب الآلي

فيروس الحاسب الآلي، هو برنامج دخيل على برامج الحاسب المعروفة، له القدرة على التداخل في نظام التشغيل للحاسبات، وهو من هذه الناحية لا علاقة بالفيروس البيولوجي "فيروس الأمراض"، ولكنه سُمي بالفيروس؛ لأنه لا يستطيع أن يعمل بمفرده، ولكنه في حاجة إلى برنامج وسيط آخر يستضيفه، حتى يكون له مفعول، تماماً مثل الفيروس البيولوجي الذي لا بد له من وسيط كي يبدأ نشاطه الفعال.

وهذا البرنامج الفيروس عند تداخله مع نظام تشغيل الحاسب الآلي، يصبح هو المهيمن على الجهاز، وبالتالي يعطي أوامر مختلفة عن البرنامج الأصلي، فيستطيع، مثلاً، أن يعطي أمراً بمسح جميع البيانات الخاصة بموضوع ما ذي نوعية خاصة، ويمكنه كذلك أن يضيف برنامجاً كبيراً لا يهم مستخدم الحاسب، بحيث يشغل الجهاز بلا فائدة نوعاً من الإرباك.

خصائص فيروس الحاسب الآلي

(أ) له القدرة على إخفاء نفسه.

(ب) يستطيع أن يعيد نفسه عشرات المرات، بمعنى، أن له خاصية التكاثر السرطاني.

(ج) له القدرة على تنشيط نفسه ذاتياً دون تدخل من الخارج.

(د) له هدف محدد، أو مجموعة من الأهداف؛ مثل التدمير، والتخريب، ويمكنه كذلك إظهار أخطاء خداعية، بمعنى، أنه ينبه مستخدم الحاسب الآلي إلى أن هناك خطأ في البرنامج، بينما لا يكون هناك أي خطأ، وذلك بهدف إحداث البلبلة والإرباك.

(2) الدودة المدمرة

هناك وسائل أخرى غير الفيروس المعروف، تُعرّض أمن الحاسبات للخطر، فعلى سبيل المثال هناك برنامج يُسمى Worm أو الدودة، وهذا البرنامج لا يحتاج إلى وسيط حتى يعمل، ولكنه يخترق نظام تشغيل الحاسبات بمفرده، من خلال ثغرة معينة في نظام التشغيل الأصلي، وإذا كان هذا الحاسب مربوطاً بشبكة مع الحاسبات الأخرى، فإن البرنامج "الدودة" ينفذ العمل التخريبي نفسه لكل حاسبات الشبكة، مستغلاً نفس الثغرة نفسها، وذلك؛ لأن نظام التشغيل عادة ما يكون، هو نفسه في كافة الحاسبات الأخرى.

(3) فيروس الحاسب الآلي سلاح جديد في العمليات الحربية

بالرغم من أنه لم يثبت حتى الآن استخدام فيروس الحاسب الآلي في الأعمال العسكرية المضادة، إلا أنه ليس من المستبعد استغلال هذا السلاح الجديد في الأعمال العدائية بين الدول خلال مراحل الصراع المسلح.

ليس من الضروري أن يكون الفيروس على شكل برنامج دخيل، ولكن يمكن أن يكون جزءاً من نظام التشغيل المصاحب للحاسب، وهذا مكمن الخطورة، خاصة للدول التي تعتمد على استيراد هذه الحاسبات ضمن أنظمة متكاملة تامة التصنيع بالدول الأجنبية، التي قد تكون حليف اليوم وعدواً مباشراً أو غير مباشر غداً.

يمكن تقسيم وسائل إدخال الفيروس، إلى أي نظام إلكتروني معين، إلى قسمين رئيسيين:

(أ) الإدخال اليدوي

يجري بالطريقة اليدوية مباشرة، بغرض التخريب، أو الإفساد باستخدام الجواسيس أو العملاء. ومع أنها تحقق الهدف المطلوب منها، إلا أن الصعوبة قد تصل إلى درجة الاستحالة في بعض الأنظمة المؤمنة تأميناً مثالياً.

(ب) البث عن بعد

وهي الوسيلة الأكثر احتمالاً في الاستخدام، ويبث فيها الفيروس من طريق إرساله عن بعد؛ خطياً أو لاسلكياً من خلال الشبكة المستخدمة في نظام الضحية، والصعوبة في هذه الوسيلة تكمن، في تصميم الفيروس الملائم لهذا

النظام، ثم طريقة تحميله على الوسط الإشاري المناسب، لكي يتم استقباله في النظام المستهدف وقبوله.

ثالثاً: تأثير النبضة الكهرومغناطيسية Electromagnetic Pulse

1. طرق اختراق النبضة للمعدات الإلكترونية

تخترق النبضة الكهرومغناطيسية الأنظمة الإلكترونية، بطرق متعددة مباشرة أو غير مباشرة:

أ. تُعد الهوائيات من أخطر وسائل التقاط التيار الكهربي الناتج عن تأثير النبضة وتمريره إلى الأجهزة والأنظمة الإلكترونية المتصلة بها.

ب. خطوط التوصيل الطويلة.

ج. كابلات التليفونات، والكابلات المدفونة تحت الأرض.

د. كابلات التغذية.

هـ. الاختراق المباشر لجسم المعدة.

و. الفتحات والشبابيك في الأنظمة، والمعدات، والمنشآت.

2. تأثير النبضة الكهرومغناطيسية على الدوائر الإلكترونية

نظراً لارتفاع مستويات الطاقة الناتجة عن النبضة الكهرومغناطيسية، عن مستويات طاقة إتلاف الوصلات Junctions، تسبب طاقة النبضة الكهرومغناطيسية تأثيرات ضارة عديدة للأنظمة الإلكترونية المعرضة، منها:

أ. عدم انتظام، دائم أو لحظي، للدوائر الإلكترونية.

ب. انخفاض مستوى الأداء، أو إحراق للمكونات الإلكترونية للدوائر، مما يسبب عطلاً مباشراً للنظم والمعدات.

ج. يحدث ذلك؛ إما بالانهيار Break Down، أو بالانصهار، أو بفتح الروابط الداخلية لدوائر الأنظمة.

التأثير التدميري للنبضة الكهرومغناطيسية، هو تأثير حراري الأصل؛ إذ يسبب انصهار الأجزاء الضعيفة في هذه المكونات.

تتأثر جميع مكونات الدوائر، والأجهزة الإلكترونية: مقاومات، ترانزستورات، مكثفات، ملفات، دوائر متكاملة، موحدات، دوائر الميكروويف، صمامات القدرة.... إلخ.

تكون المعدات التي تعمل بالصمامات المفرغة Vacuum Tubes أقل المعدات الإلكترونية تأثراً، بينما تكون التي تعمل بالدوائر الرقمية والحاسبات الآلية أكثرها تعرضاً؛ نظراً لسرعة استجابتها لأي جهود طفيفة. ويؤثر ذلك على أداء الدوائر، أو ثباتها، وذلك بانتقالها إلى ظروف تشغيل أخرى، مثل التوقف التام Cut-Off، أو التشبع Saturation.

ظهرت حديثاً أسلحة الطاقة الموجهة Directed Energy Weapons ولها التأثير المدمر نفسه.

3. تأثير النبضة الكهرومغناطيسية على انتشار الموجات اللاسلكية

أ. تسبب تشتت في المجال الكهرومغناطيسي للأرض، مما يؤدي إلى إنتاج نوع آخر من النبضات الكهرومغناطيسية.

ب. تنتج أحزمة إلكترونية صناعية تبقى لعدة شهور، حيث تؤثر جرعتها الأيونية على كفاءة انتشار الموجات اللاسلكية.

ج. تغيير مستويات الامتصاص، والشوشرة.

د. ظهور تداخلات مختلفة ناتجة عن انتشار الموجات اللاسلكية في مسارات متعددة، وهو ما يعرف بظاهرة "الخفوت" Fading.

هـ. ظهور طبقة متأينة داخل طبقات الجو العليا تبقى لعدة ساعات، أو أيام، تكون مصدراً للشوشرة، ولامتصاص الترددات اللاسلكية.

و. حدوث تداخلات على الترددات العالية جداً، وفوق العالية، فضلاً عن إضعاف الترددات المتوسطة، والعالية.

4. تأثير النبضة الكهرومغناطيسية على انتشار موجات الميكروويف

أجمعت المصادر العلمية المتاحة على أن هناك تأثيراً على الترددات الأقل من واحد جيجاهيرتز. ويحتمل أن يكون هناك تأثير محدود على حيز الترددات الأعلى من واحد جيجاهيرتز، ويضمحل التأثير كلما ازداد التردد في الحيز.

ويشترط للتأثير على الموجات الكهرومغناطيسية من النبضة الكهرومغناطيسية أن يكون التفجير النووي من ارتفاعات عالية.

رابعاً: أعمال التدمير للأهداف الإلكترونية المعادية

المقصود بتدمير المعدات الإلكترونية، هو: "القضاء، أو الاستيلاء، أو التعطيل الجزئي للنظم والوسائل الإلكترونية؛ سواء المستخدمة في نظم القيادة والسيطرة على القوات، أو المستخدمة في الكشف، والتوجيه، والتحكم لأسلحة القتال في حالة عدم جدوى فاعلية الإعاقة الإلكترونية في التأثير عليها، وعندئذ يكون التدمير هو الوسيلة الرئيسية ضد نظم القيادة والسيطرة الإلكترونية المعادية".

يستخدم في أعمال التدمير، أو الاستيلاء على مراكز سيطرة العدو، ووسائله الإلكترونية، كل من: "المدفعية، والطيران، وقوات الإبرار الجوي والبحري التكتيكي، والوحدات الخاصة، وجماعات الاستطلاع، فضلاً عن ذلك يمكن تخصيص هذه المهمة للمفارز بأنواعها المختلفة.

لا يمكن تنفيذ مهام تدمير أهداف العدو الإلكترونية بنجاح إلا في حالة معرفة إحداثيات تمركزها بدقة عالية، التي يمكن الحصول عليها من معلومات مختلف أنواع الاستطلاع.

تحدد الوسائل الإلكترونية المطلوب تدميرها، تبعاً لمكانها، ودورها في النظام الإلكتروني لسيطرة العدو على قواته، وأسلحته، ومهماته، التي تشتمل على أهم الأهداف والوسائل الإلكترونية المعادية الآتية:

1. مراكز القيادة للسيطرة والإنذار، ورادارات إدارة النيران.

2. أهم مراكز الإشارة، مراكز الإرسال اللاسلكي، المحطات اللاسلكية ومحطات اللاسلكي متعدد القنوات المنفصلة.

3. وحدات ومراكز الإعاقة الإلكترونية.

الفصل الثاني

نظم السيطرة الألكترونية في الحروب

نظم القيادة الآلية والسيطرة اللاسلكية ووسائلها وتطورها

أولاً: الحيز الكهرومغناطيسي

1. أنواع الموجات اللاسلكية

حسب طرق انتشارها، والطول الموجي لها، وتنقسم إلى:

أ. الموجات الأرضية/ السطحية

تنتشر بالقرب من سطح الأرض، وتتأثر بالقدرة التوصيلية للأرض في مسار انتشارها، ويمكن إهمال تأثير الغلاف الجوي على انتشار هذه الموجات.

ب. الموجات الفضائية

تنتشر في الطبقة السفلى من الغلاف الجوي، وتتألف من موجات فضائية مباشرة لا تتأثر بسطح الأرض، وموجات فضائية منعكسة تتأثر بطبيعة الأرض، ونوع التربة عند نقطة انعكاس هذه الموجات.

ج. الموجات المبعثرة

تنتج هذه الموجات، لعدم تجانس طبقة التروبوسفير Tropossfer ؛ إذ يصل قدر ضئيل من الطاقة في اتجاه جهاز الاستقبال، ويتأثر انتشار هذه الموجات بخواص طبقة التروبوسفير من حيث اعتمادها على الحرارة والرطوبة.

د. الموجات السماوية

تـنعكس بوسـاطة طبقـات الأيونوسـفير، ويمكـن إهـمال تـأثير الأرض، ويتـأثر انتـشار هـذه الموجـات بخـواص الأيونوسـفير، لـيلاً ونهـاراً، وخـلال الفـصول المختلفـة عـلى مـدار الـسنة، وباختلاف السنوات. الجدول الرقم 1

2. أهمية تأمين الاتصالات اللاسلكية

يُعَدّ من ضروريات الخوض بنجاح في الحروب الحديثة، وجود شبكة اتـصالات سريعـة الأداء يمكن الاعتماد عليها، لتكون همزة الوصل بين كبار القـادة وقـواتهم؛ إذ يعـي الجنـود تمامـاً، أهمية وجود مثل هذه الشبكة؛ لذلك، تكون شبكات الاتـصالات في مقدمـة الأهـداف التـي يهاجمها العدو، وقد تشن الهجمات بهدف تـدمير مراكـز الاتـصالات ذاتهـا، أو إعاقـة البـث اللاسلكي لها، والأهم مـن ذلـك، امـتلاك العـدو القـدرة عـلى التـصنّت الجيـد عـلى الرسـائل المتبادلة بين مراكز القيادة والقوات في مسرح العمليات، والعمل على فك رموزها، إن كانـت مشفرة، لتكوين صورة لنوايا الخصم وخططـه. ولمواجهـة هـذه التهديـدات يـستمر تطـوير المعدات اللاسلكية الباهظة التكاليف، التي ازداد تعقدها حتى أمكن، حالياً، التوصل بفضلها إلى اتصالات مأمونة لدرجة لم يسبق لها مثيل.

أفــرزت التكنولوجيــا المتقدمــة المــستخدمة في شــبكات الاتــصالات، ذات المــستوى العــالي مــن الأمــان، أســاليب لتطــوير قنــوات البــث آليــاً بــشكل مــبرمج، إضــافة إلى عــدد مــن الإجــراءات الأخــرى للحمايــة؛ إذ تُعَــدّ الاتــصالات ســلاحاً ســاكناً لا غنــى عنــه، لــربط هيئــات الأركــان والقيــادات بالمقــاتلين، ولتوجيــه الأســلحة ومــن

يستخدمونها، ولتوارد المعلومات عن مختلف أنشطة العـدو، وخططـه، ونوايـاه في الجبهـة بصورة شبه مستمرة، فبغير ذلك تصبح هيئات القيادة عاجزة عـن أداء مهامهـا عـلى الوجـه الأمثل. الأكثر من ذلك، فإن الوحدات المميكنة الحديثة المقاتلة باتت لا تستطيع العمل مـن دون الاتصال الدائم بين عناصرها حتى مستوى الأفراد.

يمكن القول، إذن: أن انهيار شـبكة الاتـصالات لجـيش مـا، سـتجر عليـه كارثـة مؤكـدة عـلى مستوى العمليات الحربية، علماً بأن شبكات الاتصالات في الجيوش، معرضـة دائمـاً للتـدمير. ولذلك، تدرب طواقم الدبابات السوفيتية، مثلاً، على الاتصال فيما بينها، مستخدمة إشـارات البيارق، وذلك أثناء العمل متقاربين، بينما يدرس الجيش النمساوي، حالياً، إمكانيـة العـودة إلى استخدام الجياد، لتسليم الرسائل، وما زالت بَحريّات العالم تـستخدم الإشـارات الـضوئية للاتصال، حين تعطب أجهـزة الراديـو اللاسـلكي، أو يكـون عـدم اسـتخدامها ضروريـاً، وهـذا يوضح حاجة الجيوش الماسة إلى إنشاء نُظُم اتصالات مأمونة، يعتمد عليهـا، وسريعـة الأداء، وتُعَدّ مثل هذه الأنظمة ركناً أساسياً بـين الوسـائط الدفاعيـة/ الهجوميـة للجيـوش، ولـذلك، ينبغي وضع تطويرها في سلم الأولويات الملحة.

ويؤمل أن تؤمن نُظُم الاتصالات الجديـدة، التـي يجـرى إدخالهـا إلى الخدمـة حاليـاً، سرعـة وسرية تبادل المعلومات في أسوأ الظروف الجوية إلى أن تدخل نُظُـم إجـراءات الإعاقـة عـلى الاتصالات من الجيل المقبل ميدان الخدمة العاملة.

ثانياً: الاستخدام العسكري لنظم الاتصالات

تتيح نُظُم الاتصالات الحديثة بثاً "إرسالاً"، تلغرافياً، وصوتياً، ونقل معلومات يمكن الاعتماد عليها، بشرط استخدام حيز التردد اللاسلكي بالكامل، بدءاً من مجال التردد المنخفض جداً Very Low Frequency: VLF، حتى مجال التردد فوق العالي Ultra High Frequency: UHF، خاصة في زمن السّلم؛ إذ تعمل شبكات الاتصالات بانتظام لخدمة كافة المشتركين، إلاّ أن هذا العمل المنتظم قد لا يستمر هكذا في زمن الحرب؛ إذ إن هناك عدة عوامل تؤدي إلى الإخلال بانتظام العمل؛ فمثلاً، في زمن الحرب يصبح أي نطاق ترددي مناسب من بين سائر نطاقات التردد، بدءاً من الترددات المنخفضة Low Frequency: LF، حتى الترددات العالية High Frequency: HF الشائعة الاستخدام، علماً بأن استعمال نطاقات التردد بشكل عشوائي يسبب مشكلات تداخل البث على نطاق واسع بين المستخدمين، لذا توزع الترددات مركزياً على المستخدمين لتلافي هذا التداخل.

1. نظم الاتصالات العسكرية المعقدة

أدى عدم نجاح نُظم الإجراءات المضادة للأعمال الإلكترونية المعادية ECCM في تأمين الاتصالات اللاسلكية العسكرية ضد التنصت والإعاقة اللاسلكية المعادية، إلى تصميم نُظُم اتصالات عسكرية معقدة، أكثر تقدماً، صُممت طبقاً لأحدث التقنيات، باستخدام المعالجة البيانية للحاسبات الآلية، والتي تتميز بتعقد نُظُمها الإلكترونية، غير أنها عالية النفقات.

وقد بات تصميم نُظُم الاتصالات العسكرية الحديثة يواجه التحديات باستخدام نُظُم مدمجة في غاية التقدم، لخفض احتمال الاعتراض "التنصت" :Low Probability Intercept LPI، فضلاً عن معدات مقاومة الإعاقة Anti Jamming: AJ، وبينما كان تركيب نُظُم للإجراءات المضادة للإجراءات الإلكترونية المعادية ECCM، لا يتم إلا في مراكز الاتصالات الثابتة، أو تلك المركبة على شاحنات، بدأت تظهر، حالياً، أجهزة اتصالات محمولة مزودة بأجهزة ECCM لمقاومة التنصت والإعاقة اللاسلكية المعادية.

يعتمد تصميم أجهزة ECCM لمقاومة التنصت والإعاقة اللاسلكية على:

أ. تشغيل الأجهزة اللاسلكية، سواء للإرسال، أو للاستقبال، بصورة آلية أثناء الاستخدام في ظروف الإجراءات الإلكترونية المضادة ECM "التنصت، والإعاقة الإلكترونية المعادية".

ب. مضاعفة أنواع العمل، وكذلك حيزات التردد التي يعمل من خلالها الجهاز اللاسلكي في الاستقبال والإرسال.

ج. استخدام تكنولوجيا حديثة للاتصالات، نظراً لما يميز الإرسال اللاسلكي بالأجهزة الحديثة من: "تردد قافز في نطاق ترددي متغير باستمرار، وفي زمن متغير أيضاً باستمرار، وحيز إرسال متغير بآلاف الاحتمالات"، فمن المنتظر أن تشكل هذه الخصائص مهمة صعبة لمصممي هذه الأجهزة، عند تطبيقهم مبدأي مقاومة الإعاقة، ومقاومة التنصت في هذه الأجهزة، وإن كان المختصون، حالياً، لا يركزون إلا على استخدام التردد القافز في أجهزة الإرسال

الحديثة، على الرغم من أن هذه التقنية لا توضح تماماً كيفية حماية هذا الإرسال من أعمال التنصت والإعاقة الإلكترونية المعادية".

2. نظم الاتصالات الإلكترونية لمراكز القيادة والسيطرة وتطورها

حدث تطور هائل في نظم القيادة، والسيطرة، والاتصالات، والحاسبات الآلية، والاستخبارات، Command, Control, Computer, Communication and Intelligence: C4Iبغرض ضمان تدفق سيل المعلومات لجميع القادة والقيادات على مختلف المستويات بما يمكنهم من معرفة ما يدور حولهم، وسرعة طلب الدعم النيراني؛ سواء من المدفعية، أو القوات الجوية، إلى جانب ضمان حرية العمل للقيادات، وفي الوقت نفسه العلم بما يدور لدى الجوار، كما تحقق هذه المنظومة آلية السيطرة لسرعة التعامل مع هذا الكم الهائل من الأنظمة الإلكترونية؛ لضمان سرعة رد الفعل المناسب في اتجاهات مختلفة بناء على معلومات فورية من ميادين القتال على عدة جبهات، والتي يطلق عليها أسلوب دمج/ صهر المعلومات.

3. القيادة والسيطرة باستخدام الأقمار الصناعية

تعتمد معظم دول العالم في تحقيق اتصالاتها؛ سواء المدنية أو العسكرية على استخدام أقمار الاتصالات التجارية الخاصة بها، فضلاً عن شبكة الاتصالات الدولية عبر الأقمار الصناعية، عدا أمريكا وروسيا؛ إذ تعتمد كل منهما في اتصالاتهما العسكرية على شبكة متكاملة من أقمار الاتصالات العسكرية.

وعموماً فإن أقمار الاتصالات تنقسم من حيث الاستخدام إلى:

أ. أقمار الاتصال المدنية: والمتمثلة في:

(1) الأقمار الصناعية الميدانية ثابتة الخدمة، مثل INTELSAT، وعاموس، وARABSAT.

(2) أقمار البث المباشر، مثل: نايل سات.

(3) أقمار الاتصال بالوحدات المتحركة، مثل INMARSAT.

ب. أقمار الاتصالات العسكرية

تتميز أقمار الاتصالات العسكرية باستخدامها لحيز واسع من الترددات، داخل حيز الموجة القصيرة SHF، لتحقيق الاتصال مع المراكز الثابتة والمتحركة، فضلاً عن القواعد البحرية، والقواعد الجوية، كما تتضمن العمل في حيز الترددات فائقة العلو EHF، إضافة إلى الاستخدام الموسع لأنظمة الطيف الموسع، خاصة أسلوب التهجين، والمتضمن الاستخدام المزدوج لكل من: "القفز الترددي، والتتابع المباشر"، ومن أمثلة أقمار الاتصالات العسكرية ما يلي:

(1) منظومة الأقمار الصناعية MILSAT.

(2) شبكة الأقمار الصناعية للقوات الجوية الأمريكية AFSAT COM.

(3) شبكة الأقمار الصناعية لقيادة القوات الأمريكية DSCS.

(4) شبكة الأقمار الصناعية للقوات البحرية الأمريكية FLTSAT COM.

(5) سلسلة أقمار كوزموس الروسية.

ج. أقمار الاتصال بالغواصات

من الاستخدامات المهمة والعديدة، للأقمار الصناعية، تحقيق الاتصال مع الغواصات على المستوى الإستراتيجي، باستخدام الليزر؛ إذ ترسل الإشارات، والمعلومات بمعدل إرسال سريع، ويطلق على المنظومة المستخدمة في ذلك SLC. وهي تستخدم أساساً، بغرض استكمال نظم القيادة والسيطرة الآلية، في الاتصال بالغواصات ورفع كفاءتها. ومن الملاحظ أن إشارة الاتصال المستخدمة لشعاع الليزر تتميز بالقدرة على اختراق المياه، وكذلك السرعة العالية في إرسال المعلومات، مما يجعلها ذات أهمية خاصة بالنسبة لشبكة القيادة والتحكم في الغواصات.

4. آلية مراكز القيادة والسيطرة

تمثل مراكز القيادة العنصر الأساسي لنُظُم القيادة والسيطرة، وهذه المراكز لديها القدرة على السيطرة التامة على العناصر المرؤوسة، واتخاذ القرار، مع عدم الاعتماد على المركزية المطلقة. ويتطلب هذا توافر قدر كبير من البيانات والمعلومات اللازمة لتقدير الموقف، واتخاذ القرار في الوقت المناسب. وهذا لا يتأتى إلا بالاعتماد الكبير على الحاسبات الآلية لحفظ، وتداول، ومعالجة المعلومات.

يجب أن تحقق هذه المراكز القدرة على المقاومة الشديدة للعدائيات الإلكترونية، مع القدرة الذاتية على تقليل التداخل الكهرومغناطيسي، سواء الناتج من المعدات المنتشرة في أرض المعركة، أو بين معدات الاتصال المختلفة، مع إمكانية

العمل تحت ظروف استخدام الخصم السلاح النووي، وأسلحة التدمير الشامل، مع استمرار السيطرة على الوحدات المرؤوسة، وكذلك مقاومة الحاسبات الآلية للإشعاع باستخدام الدوائر الإلكترونية الصلبة Hardened التي تقاوم الإشعاعات النووية.

ومن أهم التطورات التي تساعد على سهولة العمل وعرض المواقف، واتخاذ القرارات بل وإرسال المعلومات إلى المرؤوسين والوحدات الفرعية، وسائل العرض الحديثة التي تستخدم أسلوب عرض الموقف القتالي محدثاً آلياً عن الوحدات والأسلحة المختلفة؛ إذ ترسل الأوامر مباشرة من خلال شاشة العرض الكبيرة Large Screen Display، مع صورة كاملة لموقف العمليات إلى كافة المستويات المطلوبة.

ثالثاً: دور الحاسبات الآلية في نظم القيادة والسيطرة الحديثة

يُعَدّ عنصر القيادة والسيطرة أهم عنصر في المعركة الحديثة، وفي الوقت نفسه، يصبح، دائماً، أصعب المشكلات التي يمكن التحكم فيها، ويرجع ذلك إلى التطورات التكنولوجية الحديثة التي تحققت في مجال الحرب الإلكترونية.

وتعرف رئاسة هيئة الأركان المشتركة للقوات الأمريكية دور برنامج القيادة والسيطرة بأنه: "قيام القيادة بإنجاز أعمال التخطيط والإدارة والتنسيق والسيطرة على القوات والعمليات من خلال الاعتماد على تنظيم معين من الأفراد والمعدات وشبكات الاتصال والمرافق والإجراءات".

وتتم إدارة أعمال الحرب الحديثة والسيطرة على عمليات القتال، وفق نُظُم متطورة، لجمع ورصد المعلومات عن الأهداف ورصدها وتحليلها والتعامل معها، وهذه النظم تضم الحاسبات الآلية، والمستشعرات، ونظم التوجيه الدقيق، وللحاسبات الآلية فضل كبير في مجال تكنولوجيا الاتصال لتحقيق القيادة والسيطرة على مسرح العمليات؛ إذ تستخدم هذه الحاسبات في شبكات نقل البيانات والمعلومات من الوحدات الصغرى إلى قيادة التشكيلات، بحيث يمكن للقيادات تعرف المواقف بشكل دقيق وسريع لإصدار القرارات الفورية، بما يتناسب مع المواقف فيما ما يطلق عليه "شبكة الاتصالات الآلية للقيادة والسيطرة".

ومن خلال شبكة القيادة والسيطرة التكتيكية يخزن كل قائد ميداني المعلومات المتوافرة لديه عن وحدته وتفاصيل استعداداتها، ومعداتها، ومخزوناتها، واحتياجاتها، ليستطيع القائد في أي وقت معرفة الحالة الحقيقية لأي وحدة. وبعض البرامج تمكن القيادات من معرفة الحالات الحرجة للوحدات من خلال قيام الحاسبات الآلية بشكل آلي بلفت نظر القادة للوحدات التي تواجه مواقف حرجة.

يعتمد نجاح نظم القيادة والسيطرة على اكتساب ثقة القيادة في هذه النظم، ولا يتم ذلك إلا بمرونة أنظمة الحاسبات الآلية وقابليتها لتلبية مئات الواجبات الجانبية الأخرى، بل وإمكانية تفاهمها مع وسائل الاتصال والسيطرة وتخزين المعلومات؛ إذ إن الأجيال الحديثة من نُظُم القيادة والسيطرة تكون قادرة على تنفيذ عدد من الوظائف الجانبية، لا تقل أهمية عن المهام الرئيسية مثل:

- التحديث شبه الفوري للمعلومات عن قوات الخصم وقياداته ومتابعة نشاطها، والشيء نفسه بالنسبة للقوات الصديقة.
- تقويم الخسائر من جانب القوات الصديقة.
- توفير أي بيانات إحصائية تساعد في أعمال الإشراف والإمداد والشؤون الإدارية.

1. نظم الحاسبات الآلية لمراكز القيادة والسيطرة الآلية وتطورها

حدث تطور في استخدام الجيل الخامس من الحاسبات الآلية؛ التي تستخدم الذكاء الاصطناعيArtificial Intelligence، والجيل السادس منها الذي يستخدم الشبكات العصبية Neural Networks؛ إذ يأخذ الحاسب قراراً طبقاً للخبرة السابقة، حتى ولم تعط له قواعد أو هوامش مسبقة، وهو خطوة على سبيل تحقيق الذكاء الإنساني للحاسبات، وهذا الاتجاه الجديد بالغ السرية وتعمل فيه كل من أمريكا واليابان فقط، ولم يصرح عنه إلا في 1987 برغم وجود هذه التكنولوجيا في أنظمة أمريكية استخدمت في حرب تحرير الكويت، هذا علاوة على التطوير في استخدام الإنسان الآلي Robots.

والتطور المذهل في سرعة رد فعل الحاسبات وقدرة استيعابها، التي تنعكس بدورها على قدرة أنظمة القيادة والسيطرة، مثلاً في تطوير أسلوب اتخاذ القرار لضابط العمليات أثناء الهجوم؛ إذ تقوّم الحاسبات الآلية، التي تستخدم أحدث برمجة جاهزة Software، الموقف، ثم توصي باستخدام قوات/ سلاح معين

واضعة في الحسبان كل العوامل، والإمكانات المؤثرة، والمتاحة للقائد المناط به اتخاذ القرار.

يعدّ الاستمرار في التطوير، للوصول إلى الآلية الكاملة، وتحقيق ذلك في الوقت الحقيقي Real-Time، الشغل الشاغل لمصممي الأنظمة الحديثة؛ إذ تحقق الأنظمة الآلية من نوع ADDS، التي تستخدم لتوزيع البيانات، والمعلومات، لمتطلبات إرسال واستقبال كمية هائلة من المعلومات والبيانات، في ميدان القتال في الوقت الحقيقي.

هناك العديد من البرامج لتجميع كل أنظمة القيادة والسيطرة الآلية وتكاملها، وتحقيق إمكانية العمل، والموائمة بينها، سواء على المستوى القومي لكل دولة من دول حلف شمال الأطلسي، أو على مستوى كل الدول المتحالفة مع بعضها، خاصة في مجال المعلومات، والمخابرات، والإنذار؛ إذ بموجب هذه البرامج، مثل البرنامج الأمريكي من نوع JINTACCS، تصمم أنماط قياسية معينة Standards، وأسلوب موحد للاستخدام، والتعاون بين هذه الأنظمة، مثل توحيد المفاهيم، والاصطلاحات لكلمة معينة، أو توحيد شكل الرسالة وطولها Message Format واللغة المستخدمة، ووصلات نقل المعلومات التكتيكية Tactical Data Link، والإجراءات التي بموجبها يعدل كل فرع، أو سلاح، من مركز القيادة والسيطرة الخاص به، ليتواءم مع الأنظمة الأخرى. وجدير بالذكر أن نوعية البرمجة الجاهزة Soft Ware، تحدد، إلى حد كبير، مدى كفاءة مراكز القيادة والسيطرة الآلية.

وسعياً لتحقيق الاستمرار والبقاء لمراكز القيادة والسيطرة الآلية، تحت مختلف الظروف، بما فيها الضربة النووية، ظهرت نظم القيادة والسيطرة المحمولة جواً، مثل نظام القيادة والسيطرة والإنذار المحمول جواً Awacs، والمركب في الطائرة Sentry E-3 التي يطلق عليها اسم "الديدبان"، ونظام القيادة والسيطرة المحمول جواً E2-C، والمركب في الطائرة C-130... الخ.

ولتطوير دقة تحديد الإحداثيات للأهداف والقوات والمعدات المتحركة "خطوط الطول وخطوط العرض والارتفاع"، حتى 16 متراً والسرعة حتى متر واحد/ ثانية، ولزمن حتى 100 نانو ثانية بوساطة نظام الملاحة وتحديد الإحداثي والوقت بالأقمار الصناعية Navistar Global Positioning System.

2. نظم القيادة والسيطرة الحديثة

كان لنتائج حرب الخليج الثانية الأثر الأكبر في تحقيق ثورة في تكنولوجيا التسليح العالمي تتجاوز أبعاد ما حدث بعد حرب أكتوبر 1973؛ إذ تحولت الصحراء، والمياه، والأجواء في منطقة الخليج إلى حقل ميداني لاختبار فعالية ما تحويه الترسانتين الأمريكية والغربية من نظم تسليح متطورة، وهي نُظُم خصصت لتطويرها مئات المليارات من مخصصات ميزانيات الدفاع في هذه الدول على مدى العقدين الماضيين، إلا أن الاختبار الأول لفعاليتها قد تحددت نتائجه في ضوء ما أسفرت عنه حرب الخليج الثانية؛ إذ ثبت أن النصر في الحرب الحديثة يكون في جانب الطرف الذي لديه حرية (قدرة كبيرة) على تدفق المعلومات.

وقد حظيت نظم القيادة والسيطرة الحديثة، التي لا يزال بعضها في مرحلة التجارب بفرصة لا تعوض للعمل الميداني؛ إذ إن الحرب الحقيقية هي التي تقوّم نظم القيادة، والسيطرة، والاتصالات بين القوات المختلفة، الجوية، والبحرية، والبرية، هذا التقويم الحقيقي الذي يفوق كل أساليب التقويم والاختبار التي تضعها الشركات المنتجة لهذه النظم؛ سواء في المعامل أو في التجارب الميدانية المحدودة.

ومن بين نظم القيادة والسيطرة التكتيكية الحديثة، التي اشتركت في حرب الخليج الثانية، النظام الأمريكي Joint and Surveillance Tactical Attack Radar System: JSTARS المحمول على طائرة من نوع E-8A، ونظام Rapidly Command and Control RADIC الأمريكي، ونظام ORCHICDEE الفرنسي المحمول على طائرة عمودية من نوع "سوبر بوما".

أداء هذه النُظُم في حرب الخليج الثانية وفر على الشركات المنتجة مجهود الدعاية وتكاليفها، وأتاح لها الفرصة لتطوير نظمها، وتعديلها، للتغلب على أي مشكلات ثبت وجودها في ميدان القتال الحقيقي المزدحم بكل ما أنتجه العالم من وسائل القتال والدمار.

أ. نظام القيادة والسيطرة المحمول جواً JSTARS

استخدمت الولايات المتحدة في حرب الخليج الثانية، نظام القيادة والسيطرة التكتيكي JSTARS المحمول على طائرة E-8A التي أطلق عليها اسم "جوينت ستارز" Joint Stars. وهذا النظام مشروع مشترك بين القوات الجوية

والجيش الأمريكي بدأ العمل فيه في1985، وقدرت تكاليف المرحلة الأولى منه بحوالي 850 مليون دولار. وعلى الرغم من أن نظام JSTARS قد تم تطويره، أساساً، لصالح القوات الجوية الأمريكية والجيش الأمريكي، إلاّ إنه سيؤدي دوراً كبيراً في معاونة القوات البرية، من خلال مراقبة تحركات القوات المعادية من الجنود والتشكيلات المدرعة في العمق، وخلف خطوط القتال، وتحديد الأهداف التي يتم إصابتها بنظم المدفعية الصاروخية.

طائرة "جوينت ستارز" Joint Stars طائرة "بوينج ـ 707"، مجهزة بمعدات رادار واتصالات متطورة للقيام بمهام المراقبة الأرضية من الجو: "طائرات الأواكس تستخدم للعمليات الجوية فقط"، ويمكنها العمل إحدى عشرة ساعة متواصلة أو أكثر، بفضل إمكانية تزودها بالوقود في الجو. وتستطيع الطائرة رصد الأهداف البرية الصغيرة مثل؛ المركبات المدرعة، أو مواقع الرادار، وتحدد للقوات الصديقة أسلوب التعامل مع الأهداف المعادية.

ويجمع رادار الطائرة المعلومات، ثم تحللها الحاسبات، وتحدد الأهداف على الشاشات المخصصة لها، لنقلها إلى القادة في الميدان عن طريق محطات أرضية متحركة لتستخدم هذه المعلومات في توجيه ضربات جوية أو برية في خلال دقائق من اكتشافها. وكذلك تنقل المعلومات من النظام إلى المدفعية الصاروخية.

وقد استخدمت القوات الأمريكية في حرب الخليج الثانية، نظام JSTARS بالتعامل مع أحدث نظام صواريخ تكتيكية، وهو الصاروخ Army Tactical Missile System: ATACMS الذي يُطلق من قاذف النظام الصاروخي

المتعدد MLRS نفسه، واستخدم، للمرة الأولى، لتجربته عملياً ضمن النُظُم المتعـددة التـي استخدمت لهذا الغرض.

ب. نظام القيادة والسيطرة الأمريكي RADIC المحمول جواً

نقل سلاح الجـو الأمـريكي نظـم القيـادة والـسيطرة الـسريعة Rapidly Command and Control مـن نـوع RADIC إلى المملكـة العربيـة الـسعودية. ويـستقبل هـذا النظـام المعلومات من الطائرات الحربية، وطـائرات الإنـذار المبكـر، ثـم تنقـل هـذه المعلومـات إلى بطاريات الدفاع الجوي، ومواقع الرادار، والطائرات، والقوات البحرية، والقوات البرية.

تستطيع الجهات التي تتعامل مع النظام إضافة أي معلومات إلى الشبكة، وكذلك حذف أية معلومات. وكل ذلك يتم في الوقت الحقيقيReal Time، ويتألف نظام RADIC الذي نقل إلى الخليج من ثلاث شبكات، وكل شبكة وحدة تعمل بقدرتها الذاتيـة، ويمكـن لأيـة وحـدة مقاتلة لديها أجهزة لاسـلكية تـستخدم مـوجتيHF أو UHF، ولـديها وحـدة حـل الـشفرة الخاصة بالنظام، التعامل مع النظام، وأخذ ما تحتاج إليه من معلومات.

ج. نظام القيادة والسيطرة الفرنسي ORCHICDEE المحمول جواً

اسـتخدمت القـوات الفرنـسية في حـرب الخلـيج الثانيـة، أحـدث نُظُـم الكـشف المحمولـة جـواً، الـذي يطلـق عليـه اسـم ORCHICDEE، وذلـك لاختبـاره عمليـاً، للمـرة الأولى، في ميــدان القتــال الحقيقــي، ولمراقبــة ميــدان المعركــة. ويتكــون النظــام مــن رادار محمــــول جــــواً مــــن نــــوع AS-332، عــــلى الطــــائرات العموديــــة "ســــوبر

بوما"، للمراقبة الأرضية، ومعدات اتصال ونقل معلومات لمراكز القيادة الأرضية أو للطائرات العمودية الصديقة في ميدان المعركة.

يحقق النظام كشف تحركات القوات المعادية ومراقبتها، بعمق حتى 100 كم داخل أراضيها، إضافة إلى إمكانية استخدامه في أعمال القيادة والسيطرة على أعمال الطائرات العمودية المسلحة. ويعمل النظام على ارتفاع يتراوح بين 200 و4 آلاف متر. ويصل مدى كشف الرادار حتى 120 كم، ويمكن طي "ضم" الهوائي أسفل ذيل الطائرات أثناء عمليتي الإقلاع والهبوط، ويحقق الهوائي الكشف الدائري في جميع الاتجاهات. وقد بدأ تطوير هذا النظام في 1986، وتمت أعمال التجارب والاختبارات في 1990 في غربي أوروبا، تمهيداً لاستخدامه مع القوات المشتركة في حلف شمال الأطلسي.

3. التطور في الأنظمة اللاسلكية

أ. تقنية الطيف القفز الترددي

تعدّ تقنية استخدام الطيف القفز الترددي F.H في الاتصالات، جديدة نسبياً، وهي لا تستخدم تردداً واحداً لبث الرسائل، بل عدة ترددات موزعة على نطاق ترددي واسع تنتقى عشوائياً، وتشمل تقنية "الطيف المنفلت" أنماط بث عدة أهمها: "البث القافز، والبث في فترات متغيرة بتردد متغير النغم يطلق عليه "النظام المنغم بالزقزقة" 3CHIRPING، والبث بمزيج من تلك الأنماط".

لكن تقنية البث القافز باستخدام "الطيف القفز الترددي" هي الأكثر استخداماً وتتضمن بث التغيير عشوائياً من طريق شفرة خاصة، تتولد آلياً داخل جهاز البث، والمحطة المستقبلة في الوقت نفسه، وتتطلب تقنية البث القافز القدرة على التحكم في توقيت دقيق متزامن لعمل كل من أجهزة البث والاستقبال. وتتم في الواقع عمليات التوقيت الدقيق من خلال مقياس معياري يستخدمه المستخدم العسكري لقياس فعالية أجهزة التردد القافز وجودتها، وباستطاعة أي مرسل، أو مستقبل ضمن هذه الشبكة، أو الشبكات، أن يعمل، إما لمراقبة البث، أو مركزاً لتقوية البث، وهذه الميزة تجعل نظام الاتصالات فائق الفاعلية، وذو حظ أوفر في البقاء، فحين يدمر العدو أحد المراكز يتولى مركز آخر، آلياً، سد الفراغ، فيؤدي مهام المركز المدمر.

ويتركز التطور المنتظر في هذا المجال في زيادة سرعة التغير للترددات القافزة، وبما أن عمال تشغيل أجهزة تشويش العدو يجهلون عادة حيز التردد القافز، وكيفية تتابع البث عند الخصم، تصبح حماية البث مؤمنة لدرجة كبيرة، ولكن ذلك، لن يتحقق إلا إذا كان معدل قفز التردد، أسرع من طاقة أجهزة استقبال معدات الإجراءات الإلكترونية المضادة الخاصة بمعدات الإعاقة Electronic Counter Measures: ECM التي لا تستطيع، آنذاك، تتبع الإشارة المرسلة في أثناء حركتها خلال مشع الطيف الترددي أو الزمني. لذلك، يلزم أن ينفلت البث على أوسع نطاق ترددي ممكن، بحيث تصبح الإعاقة عليه غير ذات جدوى؛ إذ من المعروف أن الإعاقة على البث المعادي أمر صعب، ولكنه غير مستحيل، ويعتمد في نجاحه على ثلاثة أمور أساسية: "بعد جهاز الإعاقة عن

مركز البث، وعرض نطاق التردد المستخدم للبث الذي ينبغـي الإعاقـة عليـه، وأخـيراً، طاقـة جهاز الإعاقة.

بمجرد ارتياب العدو في أن الخصم يستخدم تقنيات بث منفلتة، فإنه يضطر إلى توزيع طاقة أجهزة الإعاقة لديه، لتشمل حيزات تردد أوسع من التي يعتقد أن الخصم يستخدمها في بثه "القافز"، لأن حيزات التردد المستخدمة في البث القافز تختارها أجهـزة البـث الحديثـة آليـاً، بشكل عشوائي، وهكذا تنخفض قدرة الإعاقة آلاف المرات فتفقد فعاليتها.

ب. نظم ذات احتمالية التقاط منخفضة Low Probability Intercept

وتعنـي أنهـا نظـم ذات احتماليـة تنـصت منخفـضة؛ إذ يمكـن دعمهـا باسـتخدام تقنيـة التشفير Ciphering، وعلى أيـة حـال، بـات التـشفير مـن الـضروريات، لأنـه لا يمكـن لأيـة جهـة أن تتنبـأ بنوعيـة معـدات الخـصم وقدراتـه لـشن الحـرب الإلكترونيـة المـضادة "الإعاقة الإلكترونية". ولذلك، فمن أجـل أمـن الاتـصالات، يفـترض، دائمـاً، أن لـدى الخـصم القــدرة عــلى تتبــع إشــارات البــث، ومــن ثــم، يحــرص مــصممو معــدات الإجــراءات المعاكسة للحـرب الإلكترونيـة المـضادة ECCM، عـلى أن يكـون عـدد قفـزات البـث فيهـا أكبر، ولو بقفزة واحدة One hop، عن أفضل معدات الإجراءات الإلكترونية المـضادة ECM ، أو معـدات الـدعم الإلكـتروني التنـصت/ الاسـتطلاع الإلكـتروني ESM المحتمـل، وجودهـا لـدى الخـصم، لحرمانـه مـن الإعاقـة والتنـصت عليهـا. وتجـدر الإشـارة، في هـذا الـسياق، إلى أن معدل الـترددات القـافزة تحـدده سرعـة أداء جهـاز الـتردد المعيـاري Synthesizer،

الذي يولد حيزات التردد في جهاز البث، إضافة إلى طريقة تصميم جهاز التناغم في الهوائي.

ج. نظم الاتصال من طريق ظاهرة الشهب Meteor Burst Communication

يقدر عدد الشهب، الصغيرة والكبيرة التي تدخل جو الأرض، يومياً، بما يتراوح بين 1.5 و2 بليون وحدة، وهي حين تحترق توفر "ممراً طويلاً" من الغازات المتأينة، تمتد على مسافات تتراوح بين 10 و15 ميلاً، وتبقى مكثفة لفترة عدة مئات من الجزء من الألف من الثانية، وباستطاعة هذه الممرات عكس البث اللاسلكي، تماماً كالمرآة على مساحة في حدود 20 ميلاً طولاً، و5 أميال عرضاً. وقد أكدت الأبحاث أن الحد الأقصى لاستمرار بعض هذه "الممرات" المتأينة لا تتعدّى 20 ثانية، قبل أن يتلاشى وتتوقف فترة بقاء "الممر" متأيناً بشكل مركز بعد احتراق الشهب على المناخ وحالة الطقس والمنطقة التي تستخدم فيها نُظُم الاتصال الطيفي من طريق الشهب.

أما كيفية الاتصال نفسها، فبسيطة؛ إذ تبث إحدى محطات البث VHF إشارات اختيارية على زاوية معينة بين الأفق والسمت Zenith، في اتجاه المناطق الصديقة، وتحدد الزاوية المختارة المسافة التي على الإشارة قطعها قبل التلاشي، وهنا، يُعَدّ جو منطقة الغازات المتأينة مرآة تنعكس عليها الإشارات وتلتقط مراكز الالتقاط في منطقة الاستقبال الإشارات الواردة، وقد دلّت التجارب على أنه يمكن تسجيل ما بين 70 و100 كلمة في الدقيقة باستخدام خصائص "الممر المتأين" المعروف، علمياً، باسم "بصمة القدم" Foot Print.

أما الاعتراض الوحيد على استخدام طريقـة البـث باسـتخدام "الممـر المتـأين أي مـن طريـق الشهب، فهو أن دخول هذه الأخيرة إلى الغلاف الجـوي، ومـن ثـم الاحـتراق وتوليـد "الممـر المتأين"، قد لا يحدث حين تدعو الحاجـة الملحـة إليـه، وعـلى الـرغم مـن أن فـترة الانتظـار القصوى لحدوث التأين في الجو لا تتعدى العشرين ثانية، على الأكثر، فإن هذه الفـترة، عـلى قصرها، لا تناسب المتطلبات العسكرية، ولكن إذا آل الحـال إلى توقـف شـبه كامـل لـشبكة الاتصالات من جراء الإجراءات الإلكترونية المـضادة ECM، فحتـى لـو بلغـت فـترة الانتظـار دقيقة كاملة عند الاتصال من طريق "الظـاهرة الـشهبية" فهـذا أفـضل للتأكـد مـن وصـول الرسائل الحيوية من الوحدات المقاتلة في الخطوط الأمامية وإليها. وهكذا يتوقـع أن يـصبح لنظام الاتصال من طريـق "الظاهرة الشهبية" الداعم الرئيسي في نظام اتصالات فاعـل قـد لا يتأثر بالإجراءات الإلكترونية المضادة: التنصت، والإعاقة الإلكترونية ECM.

إلا أن بعض الجيوش المتقدمة تستخدم بالفعل شبكات اتصالات ميدانيـة متعـددة أسـاليب البث والاستقبال؛ إذ تستخدم فيها معدات تقاوم الإعاقة، كـما تـستخدم الموجـات المنمنمـة "المتناهية في الصغر"، والألياف البصرية "الضوئية"، ووصلات المعلومات المتقدمة.

وبما أن هذه الشبكات ليست ملائمة لحرب تمتد على مساحات واسعة، ونظراً إلى المـشكلات المعقدة المتصلة بمعدات الاتصال من طريق "الظاهرة الشهبية"، فقد يدفع ذلك مستخدمي هذه الشبكات إلى الاعتماد، مرة أخرى، على معدات الاتصالات VHF وHF التقليدية.

د. دور "الظاهرة الشهبية" في تأمين الاتصالات

أما فيما يتعلق بمقاومة الإعاقة وخفض احتمالات الاعتراض "التنصت"، فاستخدام "الظاهرة الشهبية" للاتصالات يوفر فرص نجاح لم يسبق لها مثيل في هذا المجال؛ إذ إن تعدد قنوات الاتصال واستحالة تحديد مكان تولد "الممر المتأين" يجعلان احتمالات النجاح في الإعاقة على البث ضعيفة للغاية، ولكن البث من طريق "الظاهرة الشهبية" يتطلب إنشاء شبكة متخصصة، ومكثفة العدد من حيث معدات البث والاستقبال لمراقبة الجو، تكون على اتصال دائم، بمختلف مراكزها من طريق وصلات المعلومات، أو الكابلات، أو الاتصال اللاسلكي، وذلك نظراً إلى تعدد قنوات البث، واستحالة توقع مكان حدوث "الممر المتأين" في مناطق واسعة من الجو. وقد أصبحت مثل هذه الشبكات جزءاً لا يتجزأ من نُظُم الاتصالات الشاملة في الجيوش الحديثة.

وفي حال اكتشاف منطقة "ممر متأين" ضمن نطاق عمل الشبكة، ترسل المعلومات "البيانات" التي تحدد مكانه في الجو إلى كافة محطات الإرسال التي تكون في حاجة إليه، كما تخطر محطات الاستقبال المعنية بذلك، وبما أن مقاومة الإعاقة، مضمونة من بداية البث حتى الاستقبال ضمن الشبكات البعيدة عن الجبهة، يصبح من الممكن الإعاقة على البث وحتى اعتراضه داخل الشبكة، إذا كانت قريبة من مسرح القتال. ولذلك، يستخدم البث من طريق "الظاهرة الشهبية" في المناطق الخلفية؛ إذ يصل بشكل آمن إلى مراكز الاستقبال. وتستخدم شبكات الاتصال هذه بنجاح ومن دون إشكالات رئيسية

حتى مسافات تصل إلى 25 ميلاً بين مراكز البث والاستقبال وهو متوسط طول "الممر المتأين" أو بصمة القدم.

هـ- تطور الاتصالات في حيز التردد العالي

على الرغم من عيوب الاتصالات بالموجات القصيرة، فإنها لا تزال أكثرها مرونة، وأقلها تكلفة، لتحقيق اتصالات، قصيرة، ومتوسطة، وبعيدة المدى. ومعظم أنواع الأجهزة اللاسلكية في حيز الموجات القصيرة لا تقاوم الإعاقة، وصعبة الاستعمال، وذات معدل إرسال مدلولات بطيء.

وخلال عقد الثمانينيات من القرن العشرين الميلادي، أحرز تقدم ملموس لتحسين الاتصالات بالموجات القصيرة بالتغلب على العيوب المذكورة، ومن بين التعديلات التي نفذت استخدام الإشارات الرقمية، والقفز الترددي، إضافة إلى استخدام وحدات تعديل، وكشف Modems، والتحكم بالمشغل الدقيق Microprocessor Control، إنشاء محور اتصال لاسلكي تردد عالي: (أُنظر شكل إنشاء محور اتصال لاسلكي)

(1) إقامة اتجاه لاسلكي أوتوماتيكياً Automatic Link Establishment. ففي الماضي كان إنشاء مواصلة لاسلكية في حيز التردد العالي يتطلب مهارة عالية للمستخدم، وكذلك استخدام منحنيات "جداول" انتشار الموجات، للوصول إلى أفضل تردد لتحقيق مواصلة لاسلكية في توقيت معين، وتتيح خاصية إقامة المواصلة اللاسلكية في هذا الحيز من الترددات؛ لأنها تختار، تلقائياً، أفضل تردد، وتحدد مدى مناسبة قناة الاتصال، وتنشئ المواصلة تبعاً لذلك.

(2) تحليـل جـودة الاتـصال Link Quality Analyses LQA، بـصفة مـستمرة، بإرسـال إشارات اختبار، وقياس جودة الاتصال، ويحول، أوتوماتيكياً، الاتصال إلى القناة الأفضل، عنـد ضعف قناة الاتصال.

و. تطور الاتصالات في حيز التردد العالي جداً

انتشر استخدام أجهزة التردد العالي جداً ذات القفز الـترددي، واسـتُخدم بعـضها، مـؤخراً، في حرب الخليج الثانية، وبعض هذه الأجهزة تستخدم جزء أمن الحيز الترددي المتيـسر للجهـاز في القفز داخل الحيز الترددي المخصص للجهاز بأكملـه، ومعظـم الأجهـزة مجهـزة بإمكانيـة تشفير المعلومـات، سـواء باسـتخدام وحـدة إضـافية Add-on Code، أو وحـدات داخليـة Built- in، وأسرع هذه الأجهزة في معدل القفـز يـصل، تقريبـاً، إلى ألفـي قفـزة كـل ثانيـة، وعلى الرغم من بعض المـشكلات في تخـصيص الـترددات للـشبكات والاتجاهـات، ومواجهـة الإعاقة على حيز عريض، والإعاقة بتتبع الإشارة Jamming Follower، فقد أظهـرت أجهـزة القفز الترددي نجاحاً كبيراً في ظروف المعركة الحديثة.

وبظهور التقنيات الرقمية الجديدة، فإن الأجيال الجديدة من أجهـزة القفـز الـترددي، تتـيح مزايـا إضـافية، مثـل مرونـة التـشغيل، وارتفـاع درجـة الكفـاءة، وارتفـاع معـدل المـدلولات "البيانات"، وسرعة معالجة الإشارات الرقمية، وفي بعض الأجهزة الحديثة تتيح إمكانية إعطاء الأولوية لمكالمات واتصالات القادة.

ز. التطور في أجهزة الاتصالات اللاسلكية

إن أهـم ملامـح أجيـال أجهـزة الاتـصالات اللاسـلكية الحديثـة، والمقبلـة، هـو زيـادة نـسبة اسـتخدام المكونـات التـي تتعامـل مـع الإشـارات الرقميـة "مكونـات رقميـة" عـلى حـساب المكونات التماثلية المستخدمة في بناء هذه الأجهزة. ومن المتوقـع الوصـول إلى بنـاء الجهـاز الرقمي الكامل، كما ينتظر أن يسفر هذا التطور في تكنولوجيا تصميم الأجهزة اللاسلكية عن طفـرة كبـيرة في الاتـصالات اللاسـلكية يمكـن أن تقـارن بـالطفرة التـي حـدثت في مجـال المعلومـات، والحاسـبات، التـي واكبـت الانتقـال مـن الحاسـبات التماثليـة Analog Computers إلى الحاسبات الرقمية Digital Computers.

وضعت نظرية الاتصالات الرقمية 1948، عندما توصل علماء الاتصالات إلى أنه يمكن التعبير عن الإشارات التماثليـة "المـستمرة في الـزمن، وقيمـة الإشـارة" بوسـاطة إشـارات محـددة في الزمن، والقيمة، وإمكان استرجاع المعلومات التماثلية منها. وأهم مميزات الاتصالات الرقمية ما يلي:

(1) إمكانية تكويد الإشارات، مما سهل عملية تصحيح الأخطاء الحادثة بـسبب الـشوشرة في قنوات الاتصال.

(2) إمكانيـة التـشفير الرقمـي، ومـا يـوفره مـن مـستوى سريـة مرتفـع، بالمقارنـة بالتـشفير التناظري.

(3) إمكانية أفضل في استرجاع الإشارات.

(4) إمكانية أفضل في تمييز الأصوات.

(5) سهولة بناء أنظمة اتصالات مقاومة للإعاقة، مثل الطيف المنتشر "الموسَّع" Spread Spectrum.

(6) سهولة تداول الإشارات؛ إذ إن سيل المدلولات الرقمية، يمكن أن يتقابل مباشرة وبسهولة مع العديد من الشبكات وقنوات الترنك، وتبديل الحزم Packet Switching باستخدام أساليب تخزين المعلومات وتدفقها.

وللحصول على أكبر فائدة ممكنة من الاتصالات الرقمية، يجب تصميم، باقي أجزاء أجهزة الاتصالات، لتناسب التعامل مع الإشارات الرقمية مثل:

(1) مخلقات الترددات الرقمية.

(2) المعدلات الرقمية.

(3) المرشحات الرقمية.

(4) دوائر التوليف، والاختيارية سريعة الاستجابة.

ح. تقويم التقنيات الجديدة

يتضح مما تقدم، أن هذه التقنيات الجديدة أتاحت مقاومة الإعاقة، وخفضت من احتمالات الاعتراض، ولم يكن ذلك متيسراً من قبل، إلا أن لهذه التقنيات عيباً أساسياً، وهو أن شبكات الاتصالات التي تستخدمها لاستطاع بعضها الاتصال ببعض، إلا من خلال جهاز خاص لتحقيق هذا الاتصال.

ومن المعلوم أنه تم تطوير مجموعة من نُظُم الاتصالات العاملة بالتردد القافز على نطاقات ترددات منفلتة، ولكنها مختلفة الأنماط ولا يمكن أن تتصل

ببعضها؛ إذ إن معدل التردد القافز يتغير من شبكة إلى أخرى، كما أن زمن التردد ونمطه مختلفان.

وعلى أية حال، يتوقع أن تبرز مشكلات معقدة للاتصالات بين الحلفاء، وحتى بين مختلف أقسام القوات المسلحة في البلد الواحد، فسلاح الجو الأمريكي، مثلاً، يستخدم نظام بث المعلومات التكتيكي المشترك JTIDS، بينما تستخدم البحرية النظام الوطني لبث المعلومات التكتيكية NTDS، وكلاهما غير متلائم للعمل مباشرة مع الآخر، ولوصلهما ينبغي تأمين معدات بينية معقدة. ويعتقد أن أمر الاتصالات سيتعقد أكثر فأكثر، حين يعم استخدام نُظُم الاتصالات التي تعمل على حيزات التردد القافز في كافة فروع القوات المسلحة الأمريكية. وقد يضطر هذا التعقيد مستخدمي، أكثر نُظُم الاتصالات تقدماً، إلى ضرورة العودة إلى أسلوب التردد الثابت التقليدي تعديل التردد Frequency Modulation: FM، تعديل السعة Amplitude Modulation: AM، إذا ما اضطروا إلى استخدام معدات قديمة عن تلك المعتمدة في العتاد المتقدم.

ويتوقع المختصون أن يبلغ الارتباك ذروته في كيفية استخدام موجات الأثير بشكل أساسي في العِقد المقبل؛ إذ إن هذا الارتباك، في حد ذاته، في رأى الخبراء، يمثل الإجراء المعاكس الأفضل من بين الإجراءات الإلكترونية المضادة لمقاومة الإعاقة، والتنصت اللاسلكي.

ط. تطبيقات استخدام التقنيات الجديدة ومجالاته

بينما تقدمت الأبحاث في عدة مجالات، تم ذكر بعضها، فإن التقنيات الجديدة، والأساليب الحديثة يتم تطبيقها فعلاً، في بعض أجيال أجهزة الاتصالات الحديثة، ومن أكثر الأنظمة طموحاً، الجهاز اللاسلكي المزمع إنتاجه للقوات المسلحة الخاصة الأمريكية، والذي يطلق عليه اسم Joint Advanced Special Operation Radio-System: JASORS، وينتظر أن تفجر الأفكار التي ستنفذ في هذا الجهاز ثورة في أجهزة الاتصالات التكتيكية على جميع المستويات مستقبلاً. ومنها الجهاز الأمريكي المنتج حديثاً وبياناته كالآتي:

(1) أحد أجهزة الاتصال الحديثة التي يستخدم فيها تقنيات وأساليب حديثة، تؤمن الاتصال. وعلى الرغم من السرية المفروضة، حول برنامج إنتاج هذا الجهاز، فإن المعلومات المتسربة عنه تكشف النقاب عن الملامح الرئيسية لهذا المشروع.

(2) فقد وقع عقد بمبلغ 48 مليون دولار، بين الجيش الأمريكي، وإحدى الشركات لتمويل مرحلة الأبحاث في أكتوبر 1990، ويعتقد أنه قد تمت اختبارات الجيش الأمريكي على الجهاز في 1995، أما المواصفات الرئيسية للجهاز فهي:

(أ) الحيز الترددي: تردد عالٍ ـ عالٍ جداً ـ تردد فوق العالي.

(ب) أنواع العمل: هاتف ـ مدلولات رقمية ـ نقل الصور المتحركة "فيديو".

(ج) أنواع التعـديل: تعـديل سـعة في حيـز الـترددات فـوق العاليـة ـ تعـديل تـردد في حيـز الترددات العالية جداً.

(د) تعديل سعة حيز جانبي مفرد في حيز الترددات العالية.

(هـ) سهولة الإصلاح؛ إذ إن الجهاز مكون من وحدات يسهل استبدالها.

(و) ينتج الجهاز في عدة أشكال منها الخفيف الذي يمكن حمله باليد 18كجم، والمحمـول في المركبات 48 كجم، إضافة إلى المحطـات الثابتـة، ويمكـن تزويـد الجهـاز بوحـدات مـدلولات "بيانات"، ووحدة تشفير داخلية.

(ز) يمكن الإرسال على ومضات سريعة High Speed Burst، تزيد من صعوبة التقاطها.

(ح) ينتظر أن تتوافر بالجهاز أساليب لمعالجة الإشارات الرقمية.

(ط) الجهاز مزود بوحدة اتصال بالأقمار الصناعية SATCOM، ويمكنه إرسال صور ملتقطة من طريق آلة تصوير تليفزيونية.

نظم السيطرة الرادارية والكهروبصرية ووسائلها وتطورها

أولاً: النظم الرادارية لأسلحة القتال الحديثة

ثانياً: النظم الحرارية لأسلحة القتال الحديثة

نظـراً للتقـدم العلمـي الكبـير الـذي حـدث في أنظمـة الاسـتطلاع، والإعاقـة الراداريـة، وكـذلك في أنظمـة الإخفـاء، والتمويـه الـراداري للأهـداف، والأغـراض، الأمـر الـذي

ساعد كثيراً على تقليل فاعلية أنظمة الكشف، والتوجيه، والتنشين الراداري ضد هذه الأهداف، سواء الأنظمة الأرضية منها، أو المحمولة بحراً، أو جواً. لهذا، فقد نشطت، في السنوات الأخيرة، مراكز البحوث العلمية، لدراسة استخدام المستشعرات الضوئية، والحرارية، لاكتشاف الأهداف وتمييزها، مع تطوير أساليب المعالجة الرقمية للصور آليا Digital Image Processing حتى أمكن إنتاج أنظمة متكاملة تشمل وسائل الالتقاط، والتتبع، والتوجيه.

1. تكنولوجيا الأشعة تحت الحمراء

أدت الصدفة دوراً كبيراً في إحداث طفرة هائلة في أبحاث الأشعة تحت الحمراء وتطبيقاتها نتيجة خطأ في تقويم الألمان للموقف في الحرب العالمية الثانية، وذلك عندما زادت خسائرهم في الغواصات خلال معارك الأطلسي نتيجة لتغيير حيز تردد الكشف الراداري بوساطة الحلفاء في الوقت الذي لم يفطن الألمان فيه لهذا السبب. وهنا، انشغلت المخابرات الألمانية في تقويم الموقف والبحث عن السبب، وكانت النتيجة النهائية لهذا التقويم، أن قوات الحلفاء تستخدم أجهزة بحث تعمل بالأشعة تحت الحمراء، لاصطياد الغواصات. وكان هذا التقويم الخاطئ للموقف سبباً في هزيمة ساحقة، وفي مزيد من الخسائر في الغواصات، ولكنه كان في الوقت نفسه دفعة قوية في مجال التطبيقات العسكرية للأشعة تحت الحمراء، فيما بعد؛ إذ شهدت المراحل الأخيرة من الحرب العالمية الثانية قفزة هائلة في استخدام الألمان للأشعة تحت الحمراء، ومع التطبيق ظهرت الثغرات متمثلة في إجراءات مضادة تقابلها إجراءات أخرى في سلسلة طويلة من الفعل ورد الفعل.

أ. الأشعة تحت الحمراء جزء من الطيف الكهرومغناطيسي

يمكن القول بأن القاعدة الرئيسية الأولية لهذا النظام هي أن الأجسام ذات درجات الحرارة الأعلى من الصفر المطلق (-˚273.15م) تُعدّ مصدراً للطاقة في حيز الأشعة تحت الحمراء. ومن ثم فإن الأهداف العسكرية تُعد من الأهداف الجيدة من وجهة نظر الأشعة تحت الحمراء.

وعموماً، فإن الأشعة تحت الحمراء هي منطقة من الطيف الكهرومغناطيسي تبدأ من الحدود السفلى للون الأحمر، حتى حدود الترددات الخاصة بالميكروويف في حيز الموجات تحت الملليمترية. وهكذا، تحتل الأشعة تحت الحمراء حيز طيف يتراوح بين 0.8 و100 ميكرون، تقريباً، التي يمكن تقسيمها إلى: الأشعة تحت الحمراء القريبة، والأشعة المتوسطة، والأشعة البعيدة، والأشعة فائقة البعد.

ب. النوافذ الجوية/ الفضائية

عند انتشار الأشعة تحت الحمراء في الغلاف الجوي، تتعرض للامتصاص، وإلى التشتت؛ بسبب وجود جزئيات من بخار الماء، والأكسجين، والأوزون، وثاني أكسيد الكربون، وينتج عن امتصاص الأشعة تحت الحمراء وجود مناطق في الطيف ذات نفاذية خاصة للأشعة، ومناطق أخرى معتمة تماماً. ويطلق على المناطق التي لا يتم فيها الامتصاص تماماً اسم "النوافذ الفضائية" Space Windows، ومن هنا، قد تنشأ بعض الاختلافات في تقسيم الموجات للأشعة تحت الحمراء.

ج. الذاكرة الحرارية

تتميز الأشعة تحت الحمراء بخاصية فريدة تصاحبها، وهو ما يطلق عليه اسم "التذكر" Memorization، فطالما أن درجة الحرارة تعتمد على عامل الزمن، أثناء تناقصها بالإشعاع من الجسم إلى الوسط، فإن هذه الظاهرة يمكن الاستفادة منها، أي أن كل جسم على الأرض، يحقق ارتفاعاً معيناً في حرارة المكان الذي يوجد فيه، وتنخفض هذه الحرارة بعد ترك الجسم لهذا المكان، وتختلف درجة الحرارة طبقا لتغير الوقت في هذا المكان.

د. الأشعة تحت الحمراء، واستخداماتها في العمليات الليلية

أتاحت الأشعة تحت الحمراء الرؤية في الظلام، الأمر الذي يجعل حروب اليوم والمستقبل مختلفة تماماً عن الماضي، مما يجعل المعارك الليلية امتداداً للمعارك النهارية. وهكذا تمتد المعارك طوال 24 ساعة يوميا، ونستطيع استقراء مدلولات مهمة من ذلك، منها ما يلي:

(1) إذا كانت هناك مجموعة من الطائرات تربض على أرض ممر في أحد المطارات، فإن ظلال هذه الطائرات على الممر تؤدي إلى اختلاف في درجة حرارة مكان الظلال عن المنطقة المحيطة، فإذا فرض وأقلعت الطائرات، فإن حرارة مكان الطائرة تكون مختلفة عن باقي أرض الممر. فإذا تم التصوير الحراري بعد فترة فإنه يمكن تمييز مكان الطائرات.

(2) وهكذا فإن الكواشف الحرارية الحساسة، والحاسبات الآلية، يمكن أن تضيف فائدة خطيرة لتصوير حدث بعد وقوعه.

هـ. البصمة الحرارية

يكشف التطور التكنولوجي عن حقائق مذهلة، فإذا كان لكل إنسان بصمة تختلف عن الآخرين لبلايين البشر، فإن البصمة قد تعددت مجالاتها بالمفهوم نفسه، وهو الحصول على طريقة للتمييز بين المكونات بدقة عالية، فهناك البصمة الصوتية، والرادارية، واللاسلكية، بل وبصمة الأسنان، وعديد من البصمات التي منها البصمة الحرارية التي تتخذ وسيلة للتمييز بين المصادر الإشعاعية؛ إذ يمكن الوصول إليها عن طريق التحليل الطيفي للمكونات الإشعاعية.

ملامح البصمة الحرارية للأهداف المختلفة

تشع الأرض والمنشآت الأشعة تحت الحمراء. ولما كانت درجة الحرارة ليست مرتفعة، فإن الإشعاع يقع في الحيز البعيد للأشعة تحت الحمراء. ونظراً إلى توافر غاز ثاني أكسيد الكربون وبخار الماء بنسبة عالية، فإن النوافذ الجوية تؤثر في تحديد البصمة الحرارية للأهداف الأرضية التي تتحدد في الحيز الذي يتراوح بين 3 و5 ميكرونات للأجسام الملتهبة، والحيز الذي يتراوح بين 8 و14 ميكروناً للأجسام العادية. ولذلك، فإن الكواشف الحرارية التي تستخدم في أجهزة الرؤية الليلية، أو البواحث عن الحرارة التي تصاحب الصواريخ الموجهة، لا بد أن يتوافق حيز إمرارها مع حيز البصمة الحرارية للأهداف الأرضية.

ويمكن استخدام الأشعة تحت الحمراء في متابعة تحركات الأهداف الأرضية، كما أمكن استخدامها للحصول على صور للطائرات، والدبابات، والموانئ،

والكباري بدقة بالغة. وهكذا، فإن الدراسة الواعية للبصمات الحرارية للأهداف المختلفة توفر التعامل المؤثر معها وتوفر أيضاً الإجراءات المضادة المناسبة.

و. عمل الأجهزة بالأشعة تحت الحمراء

يمكن تمييز طريقتين أساسيتين لعمل الأجهزة بالأشعة تحت الحمراء هما الطريقة السلبية والطريقة الإيجابية:

(1) في الطريقة الإيجابية: يستخدم باعث يضيء الهدف، فترتد الأشعة من الهدف إلى نظام استشعار حراري. وفي هذا عيب؛ إذ يمكن كشف مصدر الإشعاع، وبالتالي تدميره.

(2) أما الطريقة السلبية: فتعتمد، أساساً، على الإشعاع الذاتي للأهداف، ويمثل الغلاف الجوي وسط الانتشار. ويتم تجميع الأشعة وتركيزها على أنظمة كشف، ثم يمكن الحصول على صورة للهدف.

2. تكنولوجيا التصوير الحراري

يعرف التصوير الحراري، بأنه تكنولوجيا المشاهدة الأمامية بالأشعة تحت الحمراء Forward Looking Infrared: FLIR. وقد انبثق من تكنولوجيا الاستطلاع بوساطة المسح الخطي Linear Scan باستخدام الأشعة تحت الحمراء.

ومن المتطلبات الحربية الأساسية القدرة على الرؤية في الظلام بأجهزة سلبية لا تكشف عن وجودها، وأن الغرض النهائي، دائماً، هو إنجاز المهمة بنظام

سلبي. وقد وفرت تكنولوجيا المسح الخطي وسيلة تصوير حرارية تمكن من الرؤية المباشرة في حالة الإظلام التام، بصورة مرئية تماماً، يمكن مقارنتها بالصور المرئية في التليفزيون.

وجهاز التصوير الحراري جهاز سلبي لا تنبعث منه أية إشعاعات ولكنه يستقبل الإشعاع الحراري الذاتي الصادر عن الأهداف، كما يمكنه اكتشاف بعض الأهداف المدفونة تحت سطح الأرض، أو بين الأشجار، أو داخل المباني والمنشآت؛ إذ يصعب خداعه بأساليب الخداع والإخفاء والتمويه التقليدية.

أ. هندسة الكواشف الحرارية

تؤدي الكواشف الحرارية دوراً مهماً في الأنظمة الحرارية، بل إن مدى التقدم فيها يُعد من الأسرار التي لا يمكن تداولها بسهولة. وتأخذ في درجات السرية "سرى للغاية"، فالكاشف الحراري هو "العين الإلكترونية" التي تقهر الظلام، ومن المطلوب أن يتوافق حيز الكشف الحراري مع حيز الهدف المطلوب كشفه، فالعين البشرية تكون حساسة للضوء المرئي في حيز يتراوح بين 0.4 و0.76 ميكرون، وتكون عمياء تماما بالنسبة للأشعة تحت الحمراء.

والمطلوب في الكاشف الحراري أن يكون، كذلك، على درجة عالية من الحساسية، بحيث يميز الفروق الطفيفة في الطاقة الحرارية.

ب. أنظمة الكشف الحراري

من الحقائق المعلومة أن جميع الأجسام يصدر عنها إشعاعات حرارية يمكن اكتشافها، وتصويرها بالمستشعرات الحرارية، مما يعطي صورة حرارية للجسم،

بصرف النظر عن ظروف الإضاءة، والطقس. ومن الصعب تجنب الاستطلاع الحـراري، لـذلك فإن كثيرا من الأهداف العسكرية، تُعد من الأهداف الجيدة، من وجهة نظـر الأشـعة تحـت الحمراء، هذا مع إمكانية التمييز بين هذه الأهداف عن طريق البـصمة الحراريـة لهـا. وقـد أدى استخدام خواص الإشعاع الذاتي الحراري للأجسام إلى إنتاج العديد من معـدات الرؤيـة الليلية، والاستشعار الحراري؛ إذ تجمع أجهزة الكشف، والتصوير الحراري؛ سواء الأرضـية، أو المحمولة الأشعة الحرارية الصادرة من الأجسام، وتحولها إلى صور على شريط.

وتوجد أنظمة عديدة للتصوير الحراري منها الآتي:

(1) نظـام الرؤيـة الأمـامي بالأشـعة تحـت الحمـراء المحمولـة جـواً Forward Looking Infrared: FLIR، وهو نظـام يمكـن اسـتخدامه بطـائرات القتـال، والهليكـوبتر، والطـائرات الموجهة من دون طيار.

(2) نظام المـسح الخطـي الحـراري Infrared Line Scanner: IRLS؛ إذ يبنـي صـورة عـن الهدف من خلال عملية مسح المنطقة، ويوجـد هـذا النظـام بطـائرات الاسـتطلاع، وبـأقمار التجسس، ومراكز الاستطلاع والمراقبة الأرضية، ويحمّل على بعض القطع البحرية.

وبشكل عام، فإن مدى الكشف، ومجال الرؤية لنظم الكشف والتصوير الحراري محـدودان في اتجاه مصدر الإشعاع.

ج. أنظمة التوجيه الحراري

تتميـز نظـم التوجيـه الحـراري بخاصـية "اطلـق وانْـسَ" Fire And Forget مـع إمكانيـة الاستخدام في مختلف الظروف، خاصـة الظـلام الحالـك، بالمقارنـة بـنظم التوجيـه البـصرية. ولاستخدام هذه النظم الحرارية في توجيـه الـصواريخ، يلـزم تـوافر معلومـات ابتدائيـة عـن الأهداف "مسافة ـ اتجـاه"، وتعـدّ هـذه المعلومـات باسـتخدام رادارات القـصف والتنـشين المحمولة جواً، أو باستخدام رادارات التوجيه الأرضية/ البحريـة، وبالتـالي فـإن معظـم نظـم التوجيه الحرارية توجد في رؤوس الصواريخ، وتستخدم في المرحلة النهائية للتوجيه.

تندرج أنظمة التوجيه الحراري للصواريخ تحت قسمين رئيسيين:

(1) التوجيه الحراري بدون صور Non Image IR.

(2) التوجيه الحراري ببناء الصور Image IR- IIR.

يستخدم التوجيه الحراري التقليدي في رؤوس الصواريخ، نظراً لوجود تباين حراري كبير بـين الهدف، والخلفية المحيطة به، وفي هـذا النـوع مـن التوجيـه يقـبض عـلى الهـدف في اتجـاه الإشعاع الحراري الكبير الصادر عن الأهداف باسـتخدام تليـسكوب صـغير مـصمم لتجميـع، الطاقة الحرارية اللازمة لدقة عمل المستشعر الحراري المركب في رأس الصاروخ، وتركيزها.

يُعـد التوجيــه الحــراري ببنــاء الــصورIIR، هــو أكــثر تكنولوجيــا الاســتشعار الحــراري تعقيـداً، ويـستخدم عنـدما يكـون التبـاين الحـراري بـين الأهـداف الخلفيـة المحيطـة بهـا، صـغير نـسبياً، مثـال ذلـك الأهـداف الأرضـية. وهـذا النـوع مـن التوجيـه، آلـة تـصوير تليفزيونيــة حراريــة، موجــودة بــالرأس الباحثــة للــصاروخ، تبنــي صــورة حراريــة

متكاملة للهدف، وباستخدام تكنولوجيات المعالجة الرقمية للصور صار الحصول على صـور حرارية تفصيلية عن الهدف ممكناً.

د. الصواريخ الحرارية

استخدمت الصواريخ ذات التوجيه بالاستشعار الحراري الباحثة عن الحرارة، منـذ سـتينيات القرن العشرين المـيلادي، حيـنما فاجـأ الثـوار الفيتنـاميون الطـائرات الأمريكيـة، بالـصاروخ السوفيتي الذي يطلق من الكتف سام-7، والذي عرف باسم "استريلا"، مما تسبب في خسائر واضحة في القوات الجوية الأمريكية تم تداركها فيما بعد.

ومن هذا الجيل، ظهر الصاروخ الأمريكي "العين الحمراء" Red Eye، ثم تبعـه جيـل شـابرال Shapral، وسام-7 المعدل، وسام-9. وظهرت كذلك، الـصواريخ الحراريـة المـضادة للـدبابات تاو Tow، وهوت Hot وهكذا، ظهر تهديد جديد للأنظمة والمعدات يستخدم الأشعة تحت الحمراء في اصطياد أهدافه.

والأساس في الصواريخ الحرارية هو الرأس الباحثة Head Seeker التي تتكـون، أساسـاً، مـن ثلاث مجموعات، هي:

(1) مجموعة البصريات: وتمسح، الإشعاع الحراري الصادر من الهدف، وتجمعه وتركّزه.

(2) السبيكة: ومهمتها تقسيم هذا الإشعاع المستمر، ميكانيكياً، لتحويله إلى نبضات مشفرة، تنقل إلى الجزء الحساس.

(3) الكاشف بالأشعة تحت الحمراء Infrared Detector: ومهمته تحويل هذه النبضات إلى أوامر توجيه للصاروخ، ليتتبع الهدف.

ولا بدّ من تحقيق التوافق بين حيز الكواشف الحرارية، مع البصمة الحرارية للهدف المعادي سواء كان طائرة، أم دبابة، وعندما تزداد حساسية الكواشف الحرارية، فإن ذلك يساعد على التعامل مع الطائرة من جميع الاتجاهات؛ سواء أثناء اقترابها، أو ابتعادها، أو من الجوانب، مما يتيح التعامل مع الهدف من جميع الاتجاهات، وهذه الميزة افتقدتها الأجيال الأولى من صواريخ سام –7، ثم أمكن تداركها، فيما بعد، في الأجيال المتعاقبة: سام -7 المعدل، وسام -9، وسام -13.

وظهرت أهمية وجود أنظمة للتعارف Identification Friendly or Foe: IFF حتى يمكن التأكد من هوية الهدف، درءاً للأخطاء، وتجنباً لإصابة الأهداف الصديقة. وتركب أجهزة التعارف على القاذف، كما في الصاروخ الأمريكي ستنجر الذي يمتاز، كذلك، بحساسية فائقة علاوة على ميزة المستشعر الثنائي Dual Sensor؛ إذ يمكن تمييز جزء من الإشعاع واستقباله في حيز الأشعة فوق البنفسجية التي تصاحب الطائرات المعادية، ومن هنا يتأكد من الهدف الحقيقي المعادي، فيصعب بذلك خداع الصاروخ، مما يزيد الصاروخ ذكاء.

هـ. الصواريخ الذكية

تتميز الصواريخ الحرارية الحديثة المستخدمة ضد الطائرات، أو المستخدمة ضد الدبابات، بتزويدها برأس باحثة Head Seeker ذكية Smart، كما في الصاروخ الأمريكي "ستنجر" Stinger Post . إذ ينفذ الاستشعار في حيز الأشعة تحت الحمراء، وحيز الأشعة فوق البنفسجية، الأمر الذي يصعب معه الخداع التقليدي.

كما تتزود الصواريخ، كذلك، بمشغلات دقيقة، وذاكرة تفرق بين سرعة الهدف الحقيقي، والهدف الهيكلي، وكذلك بين كمية الإشعاع المفروض وصولها من الهدف الحقيقي إلى المستشعر على مسافات مختلفة. فإذا فرض أن الهدف الهيكلي كان ذا إشعاع أكبر من الهدف الحقيقي، فيتجنبه الصاروخ المتألق BRILLIANT، ويتجه نحو الهدف الحقيقي، ويظهر ذلك في المشروع الأمريكي Assault Breaker؛ إذ يحمل الصاروخ الرئيسي عدة حمولات فرعية إلى منطقة تجمع مدرعات معادية؛ إذ تنطلق كل حمولة فرعية إلى دبابة فتدمرها. فإذا تم تدمير دبابة زاد مستوى الإشعاع الحراري الصادر منها، عما هو مخزن في ذاكرة الحمولة الفرعية الأخرى، فلا تتجه إليها، بل تنتقي دبابة لم تتم إصابتها من قبل.

و. الأنظمة الحرارية الملاحية

إن الاتجاه الحديث، هو إنتاج أنظمة متكاملة تفي بجميع مهام الملاحة الجوية في مختلف الظروف الجوية، الليلية، والنهارية، وعلى جميع الارتفاعات، لتحقيق

أداء ملاحي متقدم. وقد استغلت التطورات التي حدثت في النظم الحرارية في أعمال الملاحة الجوية، لإعطاء صور حرارية عن الأرض محل الطيران في مختلف الظروف الجوية مع عرض هذه الصور على شاشة عرض علوية أمام الطيار.

والتطور المنتظر، هو تجهيز جميع طائرات القتال، وطائرات الهليكوبتر، والطائرات الموجهة من دون طيار، بأنظمة رؤية ليلية حرارية، لأغراض الملاحة نظام الرؤية الحراري الأمامي FLIR.

ثالثاً: أجهزة الرؤية الليلية/ الكهروبصرية/ الأشعة تحت الحمراء

إن أي قوة تمتلك تكنولوجيا للرؤية الليلية تتمتع بمزايا عظيمة، وقد برز ذلك خلال حرب الخليج الثانية في 1991، عندما استخدمت الولايات المتحدة الأمريكية، وغيرها من دول التحالف مثل هذه التكنولوجيا بكثافة، وعلى الرغم من أن التقنيات لتكنولوجيا الرؤية الليلية في ميدان القتال لبعض المتنافسين كانت مختلفة، فإن لكل منها ما يتلاءم مع ظروف البيئة. فمكثفات الصور Image Intensifiers التي تزود بها نظارات الرؤية الليلية Night Vision Goggles NVG، وأجهزة تصويب البنادق كان لها الأثر الأكبر، والفاعلية في إصابة الأهداف بدقة في ميدان القتال ليلاً.

1. الأجهزة العاملة بالأشعة تحت الحمراء

الإلكتروبصريات Electron Optics، كما يدل الاسم عليها، هي تزاوج بين البصريات، والإلكترونيات التي صُممت لتحويل الإشارات الضوئية إلى إشارات

إلكترونية صالحة لاستعمالات أخرى. ويكمن الفارق الرئيسي في الأنظمة التي تستغل الحزمة المرئية "إلكتروبصريات"، أو الحزمة غير المرئية "الأشعة تحت الحمراء"، والتكنولوجيتان كلتاهما معنيتان بالبحث في الصور التي تولد إشارات كهربائية عن طريق دفع الإلكترونات من مستوى طاقة إلى آخر.

يبحث الجهاز البصري عن إشعاع منعكس من الجسم، وعادة لكونه ناتج من ضوء الشمس، أمّا أجهزة تكثيف الضوء فتستخدم الضوء المنعكس من النجوم أو القمر؛ لتعطي رؤية ليلية سلبية. وتتراوح الأطوال النموذجية للموجة بين 0.4 ميكرون و1.2 ميكرون، أمّا الأجهزة الباحثة للأشعة تحت الحمراء فمعنية بشكل رئيسي بالحرارة الصادرة عن الهدف، وهي تتراوح بين العمود الساخن لغاز العادم الصادر عن مدخنة أو ماكينة، وحرارة جسم الإنسان على مسافة قصيرة نسبياً.

والأجسام التي تفوق حرارتها حرارة محيطها، تصدر حرارة بدرجة معينة، ويختلف طول موجة الإشعاع الحراري التي تصدر من هدف لآخر. فبمقدار ما يكون الهدف أكثر سخونة يكون طول الموجة أقصر.

إن التقنيات المستعملة في التصوير الحراري هي أيضاً متطورة على عدة مستويات. فالأجهزة التي تستخدم مركز المستوى البؤري مع عدد كبير من العناصر الكاشفة، تحقق مستويات رؤية حرارية ذات قيمة لهذه النظم، ومن هذه الأنظمة نظام الرؤية الليلية من نوع TOGS المزودة به الدبابة البريطانية تشالنجر -1 CHALLENGER-1 ومن أهم نظم التصوير الحراري من الجيل الثاني هو نظام SYNERGY الذي بدأ في 1992؛ مستخدماً عنصر كشف

X2884 الذي طورتـه شركـة SOFRADIR في فرنـسا، وقـد صـممت الوحـدات لـكي تـوفر الخدمة الطويلة، والتكلفة القليلة، والحجم الصغير، واستهلاك قليل للطاقة مع أداء عالٍ.

أدخلـت شركـة طومـسون THOMSON-CSF" تقنيـة SYNERGY في آلاتهـا للتـصوير الحـراري: "كـاترين CATHERINE، و"سـيلفي SYLVI"، و"صـوفي SOPHIE"؛ فكـاترين اعتمدت للاكتشاف الطويل المدى، ولمراقبـة النـيران في عربـات القتـال المدرعـة، وفي أنظمـة الصواريخ أرض/ جو، واسـتعملت "سـيلفي" في نظـارات القيـادة، وركبـت في الدبابـة لـوكلير LECLERC من إنتاج شركة "جيات أندستريز GIAT INDUSTRIES"، أمّا صوفي الخفيفة الوزن المخصصة أساساً لاستعمال المشاة، فقد جهـزت بهـا العربـات المدرعـة الخفيفـة مثـل GIAT AMX-10RC، أو "الفيس سكوربيون ALVIS SCORPION".

كان هدف الجيش الأمريكي في الجيل الثـاني مـن الرؤيـة عـن بعـد العاملـة بالأشـعة تحـت الحمـراء Forward Looking Infrared: FLIR؛ هـو تحقيـق أداء متطـور بأقـل تكـاليف. ويضم هذا البرنامج عائلة من أنظمة المسح العاملة على نطاق يـتراوح بـين 8 و12 ميكرونـاً، والمستخدمة في نظام سادا -2 SADA-II المتضمن نظام كشف عناصر من X4804، وسـوف يطبق الجيل الثاني FLIR في مناظير عدة مثل: "أنظمة التـصوير الحـراري في الدبابـة أبرامـز ABRAMS M1-A2، وفي الطائرة العمودية AH-64 APACHI وغيرهما".

2. أجهزة الرؤية العاملة بتكثيف الصورة Image Intensifiers

نظراً لأنه كان من السهل كشف الأجهزة العاملة بالأشعة تحت الحمراء، اقتضت الحاجة استخدام أجهزة سلبية لا تصدر أي نوع من الإشعاع، فاتجهت الأنظار إلى طيف الضوء المرئي، وإلى حزم الأشعة تحت الحمراء القريبة. ولهذا استغلت مصادر الإضاءة الطبيعية؛ كالقمر، والنجوم، والأشعة تحت الحمراء الناجمة عن الأجسام كافة، التي تشع حرارة مولدة منها نفسها، أو منعكسة عنها. وكان من النتائج التي تم توصل إليها هو أن مكثف الضوء الذي يحول الضوء إلى شحنات كهربائية، يعيد تحويلها إلى ضوء مرئي للعرض على شاشة فلوريسنتية Fluorescent Screen.

ومن أحدث منتجات أجهزة الرؤية الليلية بتكثيف الصورة ما يلي:

أ. طورت شركة ITT نظام الرؤية الليلية AN/AV-8 المركب على خوذة الطيار.

ب. أما شركة ليتون LITTON فتتابع عملها على الجيل الثالث، وتطور صمام الجيل الثاني العالي الدقة، ويتضمن لوحة القناة الدقيقة مع زيادة قوتها.

ج. من جهة ثانية يتابع الجيش الأمريكي بحثه عن التطور في مكثفات الصور؛ لذلك عمدت القيادة المركزية للجيش الأمريكي CECOM إلى طلب جهاز مراقبة، وتحكم في النيران ليلاً ونهاراً ليستعمل من قِبَل القوات الخاصة على بنادق قناصة ثقيلة، ومتوسطة، وللاستطلاع الإستراتيجي والمراقبة. وسيتضمن

هذا الجهاز صمام الجيل الثالث، ويوفر رؤية مباشرة تسمح للقناص المراقبة في الليل كما في النهار.

هناك عدة تقنيات مرشحة لتكون قاعدة صمام نظام الجيل الرابع، ومن بين هـذه التقنيـات صمامات ذات مهبط ضوئي يوسع الجواب الطيفي إلى 1.6 ميكرومتر، واستخدام أجهزة تكبير حديثة.

يعمل المكتب الأمريكي للأبحاث البحرية، وأنظمة القيادة البحرية الجوية على تقنية جديدة لنظام رؤية ليلية ملونة، يسمح للطيار استبدال نظاراتـه القديمـة للرؤيـة الليليـة بمسـتشعر متعدد الطيف ذي رأس دوار مركـب عـلى الخـوذة، ويـوفر هـذا التـصميم الرؤيـة المبـاشرة للخارج من خلال مكثف للصور يستخدم لتحويل مخرجات الصمامات إلى إشارة فيديو.

3. إسرائيل والأشعة تحت الحمراء

توظف إسرائيل كافة التطورات التكنولوجية، تحقيقاً لمبدأ البقاء، الذي يمثـل عنـصراً أساسـياً من العقيدة القتالية لها. وقد اتجهت مبكراً إلى مجال الكهروبصريات، وأولت الأشعة تحـت الحمراء اهتماماً خاصاً. كـما طـورت إسرائيـل، كـذلك، بعـض الكـاميرات الحراريـة الـصغيرة، للاستخدام على الطائرات الموجهة من دون طيار RPV، لكشف أرض المعركة ليلاً.

تـسبب الحظـر الأمـريكي المؤقـت، ذات مـرة، عـلى صـفقة صـواريخ جـو/ جـو سـايد ونـــدر الحراريـــة في تحقيـــق إسرائيـــل طفـــرة في مجـــال الأشـــعة تحـــت الحمـــراء

وتطبيقاتها؛ إذ توصلوا إلى الصاروخ شفرير جو/ جو، ثم PYTHON-3 الذي يُعَدّ، أساساً، لتطوير جيل جديد ومتفوق من الأسلحة الذكية.

وتأكيداً للعقيدة الإسرائيلية في أهمية القتال الليلي، فإنها تطور إمكانات القتال الليلي للدبابات بتجهيزها بأجهزة تصوير حراري ضمن أنظمة الرؤية للسائق، وأنظمة قيادة النيران في تكامل مدروس مع أنظمة تقدير المسافة بأشعة الليزر. وتدعم إسرائيل دباباتها بأنظمة للإعاقة الحرارية، لتحييد عمل الصواريخ الحرارية المعادية مع استخدام أنظمة دخان حديثة لها القدرة على الإخفاء، بما تمثله من امتصاص وتشتيت للأشعة تحت الحمراء. كما تطور إسرائيل، كذلك، الطائرة F-16، لمهام العمل الليلي بتزويدها بنظام Low-Altitude Navigation Infrared for Night: LANIRN للملاحة الليلية على الارتفاعات المنخفضة بالأشعة تحت الحمراء.

ومع التقدم الإسرائيلي الملحوظ، فإنها تحاول تطوير معظم القذائف التقليدية، لتكون موجهة بالأشعة تحت الحمراء.

وتطور إسرائيل قذائف الهاوتزر 100 مم، لتحمل الواحدة ثلاث شحنات فرعية مزودة بمستشعرات ملليمترية وبالأشعة تحت الحمراء يمكنها تدمير ثلاث دبابات في آن واحد.

4. بعض أمثلة أجهزة الرؤية الحديثة

أ. نظام ACTIS

أنتجت شركة CHARTER IND السنغافورية جهاز رؤية ليلية؛ للاستخدام من قِبَل أفـراد المشاة والعمليات الخاصة، وهو من النوع الحراري، ويـستخدم في أعـمال البحـث والمراقبـة وغيرهما. ويعمل في حيز يتراوح بين 8 و12 ميكروناً، مـع تـوفر مجـال للرؤيـة بـين 7 درجـة عرضاً و3.5 درجة رأسياً، ويحقق مدى رؤية 30 متراً.

يستمد هذا الجهاز تغذيته من أربع بطاريات كبيرة الحجم، ويبلـغ وزنـه حـوالي 4.6 كجـم، وأبعاده 24.7×19×13.5 سم، ومن الجـدير بالـذكر أن الجهـاز يتميـز بنظـام تبريـد داخـلي لصمام الأشعة تحت الحمراء.

ب. نظام AN/VAS-3

من المألوف بالنسبة للآليـات المدرعـة الحديثـة دبابـات، وعربـات مدرعـة، ومـدافع ذاتيـة الحركة، هو تزويدها بنوعين من أنظمة الرؤية الليليـة؛ واحـد يعمـل بمبـدأ تكثيـف الـضوء ويستخدمه سائق المدرعة، بيـنما يعمـل الآخـر وفـق مبـدأ الرؤيـة الحراريـة الأشـعة تحـت الحمراء، ويستخدمه الرامي وقائد المدرعة.

طـوّر منظـار القيـادة الليليـة AN/VAS-3 العامـل بالأشـعة تحـت الحمـراء؛ بهـدف اســتخدامه في الــدبابات أبرامــز M1-A2، والعربــات المدرعــة بــرادلي BRADLY، وLAV-25، والمــدفع الــذاتي الحركــة M-109 بــشكل يجعــل الــسائق قــادراً عـلى الرصـد، والرمـي بالرشـاش المـوازي؛ إضـافة إلى مهمتـه الأساسـية، ويـزن النظـام

12.7 كجم، ويعمل ضمن إطار الطيف الضوئي من 7.5 حتى 12 ميكرون، ويتضمن 60 لاقطاً للكشف الحراري.

ج. نظام FORMS

انتشرت أنظمة الرؤية الليلية الصغيرة الحجم، التي أطلق عليها اسم الجيب Pocket؛ للاستخدام مع أفراد الاستطلاع، والقوات الخاصة، وزود بعضها بوحدة قياس المسافة بأشعة الليزر.

تجري الولايات المتحدة الأمريكية تجارب نهائية على الأنظمة التي نهائية، قبل تسويقها، ومنها ما يطلق عليه اسم :Forward Observer Ranging and Marking Scope FORMS، وهو جهاز صغير الحجم يستخدم للرؤية الليلية، وإضاءة الأهداف بشعاع الليزر، ويستخدمه أفراد القوات الخاصة، وأفراد أطقم الطائرات في مهام الاستطلاع والمراقبة.

يفيد استخدام مثل هذا الجهاز أطقم الطائرات في تحديد مدى الأهداف، أو إضاءتها بأشعة الليزر؛ للتعامل معها بالأسلحة الموجهة بالليزر الأرضية، كما يفيد بدرجة كبيرة في عمليات الاستطلاع الليلي القريب، أثناء تنفيذ العمليات الليلية.

د. نظام FORTIS

عرضت شركة سيمنز ألبيس SIEMENS ALBIS نظام الرؤية الليلي فورتيس FORTIS، ويستند هذا النظام على أحدث تكنولوجيات الأشعة تحت الحمراء

المدمجة مع مكونات إلكترونية حديثة، وبصريات عالية الأداء. ويبلغ وزن هذا النظام 13 كجم في حالاته العملياتية الكاملة.

ويعتمد النظام على الطيف العالي النقاوة، الذي يتطلب حقل رؤية يسمح بالمسح، ومن ثم تتبع الهدف عن قرب بمدى يصل إلى عدة كيلومترات. وقد أُعتمد الجيش السويسري على نظام فورتيس من قِبَل الجيش، لما يتمتع به من قدرات على اختراق الضباب، والدخان، والغبار، وأكثر العوائق التي تبرز في ميادين المعارك، وأعمال المراقبة.

على الرغم من النوعيات القوية من المكثفات وأجهزة التصوير، لكن تبقى هذه المعدات دقيقة نسبياً؛ إذ ينبغي استخدامها بحذر، وبخاصة آلات التصوير البصرية، فعدسات التصوير ـ بشكل خاص ـ تُصنع من مادة رقيقة يسهل خدشها برمال الصحراء إلى درجة تغدو معها غير صالحة للاستعمال، كما ينبغي تنظيفها بحذر وبخاصة في حالة عدسات أجهزة التصوير على المركبات.

الفصل الثالث

التموية والخداع الالكتروني

التمويه والخداع

كان التمويه والخداع من ضمن الغرائز الفطرية التي صاحبت بعض الكائنات الحية التي استخدمتها بأشكال متعددة وبنسب متفاوتة في الصراع من أجل البقاء أو السيطرة،فتعددت وسائلها الفطرية من الاختباء متقمصةً أو خائفة إلى التمويه متلونة بشكل المكان الذي تقف عليه ولقد أثبتت الدراسات من خلال المتابعة والرصد إن الكائنات الحية الأضعف تبرع في ممارسة أساليب التمويه والخداع لتقوية مركزها في الصراع ضد الكائنات الأكثر قوة منها،فمع توالي الحقب الزمنية المتعاقبة على الحياة البشرية إستخدم الإنسان وسائل التمويه والإخفاء في حياته البدائية فاستعان بوسائل تمويه و إخفاء بدائية ليسهل من خلالها عمليات صيده للحيوانات الطريدة والتي كان لها أن بادلته نفس الاستخدام لنفس التقنية التي فيما بعد كنت بمثابة معلم للإنسان ألهمته إلى استخدام وسائل إخفاء وتمويه استنبطها من تلك المخلوقات التي ألهمت فكر الإنسان لتبين له محدودية علمه وتبرهن له في نفس الوقت على قدرة الخالق القدير الذي ضرب للإنسان مثلاً في مخلوقاته المتعددة من حيوانات ليستفيد ويتعظ.

الحرب خدعة

إنتقل استخدام وسائل التمويه والخداع من الممارسة المنبثقة من ردود الفعل الفطرية التلقائية إلى الابتكار والدراسة من خلال استثمار العقل البشري وخصائص الدهاء الإنساني الذي تعمق وأنجز في ميادين الحرب ليشكل مجموعة من المراحل المتجددة والمتطورة في استخدام التمويه والخداع في

الحرب،وفي التاريخ القديم نسبت أول استخدامات عسكرية للتمويه والخداع في الحرب إلى القدماء المصريين الذين استخدموها بأشكال عدة سواءً في حربهم أو سلمهم، والكل لا يجهل قصة حصان طروادة الشهيرة والذي عندما يئس الإغريق في حصارهم لطروادة تظاهروا بأنهم على وشك إنهاء الحصار ومغادرة المكان، وكانت بعض سفنهم قد أبحرت لكنها توارت خلف جزيرة قريبة، لجأ الإغريق إلى استخدام الخداع كوسيلة للنصر حيث بدأت الفكرة بصناعة حصان ضخم من الخشب يدخل في تجويفه مختبئين مجموعة من فرسانهم الشجعان الأشداء بحيث يقدم بالحصان إلى أسوار طروادة فعندما رأوا الطرواديون الحصان العملاق ظنوا أن إلههم قد أهداهم هذا الحصان فسحبوه إلى الداخل وأدخلوه المدينة فخرج منه المحاربون الأشداء الذين فتحوا لإخوانهم أسوار المدينة وكان لهم الفضل في إحراز النصر،هذا ما يذكرنا دائماً بأهم مبدأ عرفه التاريخ في الحرب وهو (أن الحرب خدعة).

وفي التاريخ الحديث لعل أول مرة استخدم فيها التمويه كانت في الحرب العالمية الأولى (1914-1918) حين زادت الطائرات من قدرات المتحاربين على مراقبة وكشف مواقع العدو، ولعل أشهر الأمثلة على ذلك هي قصة أحد الطيارين الفرنسيين الذي كان يحلق بطائرته فوق أحد السواحل فلاحظ أن قوارب الصيادين من احد الجوانب واضحة للعيان ومن الجانب الآخر رأى أشياء غير واضحة فعندما هبط ذهب إلى الساحل ليتأكد منها ماذا تكون فعندما وصل لاحظ أن شباك الصيادين كانت ممدودة على طول القوارب الأمر الذي جعل رؤيتها من الأعلى غير واضح فمن هنا ظهرت فكرة استخدام الشباك

كوسيلة دفاعية للتمويه والخداع منذ ذلك الوقت حتى الآن، أما في الحرب العالمية الثانية (1939-1945) فقد استخدم التمويه، بدءاً من ارتداء الجنود للملابس البيضاء في المناطق القطبية والخضراء في الغابات، إلى إخفاء المدن تحت ستار من الدخان ولقد لمست معظم الدول الحديثة أهمية وسائل الإخفاء كسلاح فعال فاستعانت به بمقاييس كبيرة في الحرب العالمية الثانية فقبل نشوب الحرب ضللت روسيا العالم بإنفرادها سياسياً ملتزمةً الصمت بُغية التمويه والخداع لكي لا تنكشف حقيقة قواتها التي ظلت لغزاً محيراً لدول العالم، ومن وسائل التضليل المتعددة التي استخدمتها عندما أطالت المفاوضات بينها وبين حلفاء الغرب والتي كانت لكسب الوقت والمسافة للاستعداد لمقابلة الألمان فيما بعد، ولما كشفت ألمانيا ضعف الحلفاء زادت الطرفين تضليلاً وذلك عندما استعانت ببعثة عسكري ألمانية لتنظيم الجيش الروسي والذي عرضت حينها عليه مجموعات أفراد غير مدربة تحمل أسلحة عتيقة لتضلل بذلك عن حقيقة تسليحها كما تمادت في وسائل الخداع حيث اشتبكت مع فنلندا الدولة الصغيرة في حرب طويلة أظهرت من خلالها أنها ضعيفة أمامها،وبذلك التمويه والخداع وضعت ألمانيا خططها العسكرية على أساسه الخاطئ فهاجمت الحلفاء أولاً وبعد أن استنفذت جهوداً كبيرة اشتبكت مع روسيا وحدث ما يعلمه الجميع من هزيمة ألمانيا النهائية.

أساليب التمويه و الخداع في الدفاع الجوي

دخلت أساليب ووسائل الخداع والتمويه ضمن خطط التكتيك العملياتي لأنظمة الدفاع الجوي لدعم الهدف الرئيسي وهو التصدي والإيقاع العدو الجوي المعادي

من خلال خداع وتضليل وسائله الاستطلاعية وإعاقة وسائلها الخداعية المحمولة جواً والصواريخ المضادة للإشعاع، وتعد عمليات الخداع والتمويه من ضمن الأعمال الهندسية التي صنفت كأحد فروع الهندسة العسكرية من ناحية المفهوم الشامل في معظم فروع الوحدات القتالية العامة ولكن عندما تستخدم عمليات التمويه والخداع في أحد فروع القوات المسلحة فأنها تدخل ضمن إطار التكتيك، إذا فالخداع والتمويه في الدفاع الجوي هو عمليه تكتيكيه دفاعية.

الطرق الأساسية لعمليات التمويه والخداع :

-التخفي : وهو عملية إخفاء الهدف بشكل كامل وتعني عدم إظهار أي ملامح شكلية توضح أي معلم أو جزء منه.

-المزج :وهو عملية تمويه الهدف ومزج ملامحه الشكلية مع طبيعة الأرض الموجود عليها بحيث لا يمكن التمييز بينهما.

-الخداع : وهو عملية بناء هياكل أو وسائل كاذبة تشابه من حيث الشكل للنماذج الحقيقة وتسمى مواقع خادعة.

وتبنى عملية التمويه والإخفاء والخداع على مجموعة من الشروط التي تبدأ عند اختيار موقع التمركز مباشرة، فبعد الانتهاء من تحديد أماكن المعدات والأفراد تبدأ مباشرةً عملية الإخفاء وذلك حرصاً على عدم معرفة أو اكتشاف العدو لمكان الموقع، وأن الحرص على عدم انتظام الموقع شرط أساسي لنجاح عملية التمويه، كما يجب دمج الأفراد بطبيعة الأرض بوسائل التمويه السابق ذكرها حيث من المعروف أن الرامي أو الراصد في ظروف المعركة قد يضيع الهدف

بعد رؤيته أو الرامي عليه، وكذلك عندما يكون الهدف مموهاً أصبح الاهتداء إليه من جديد يتطلب زمناً قد يسمح للهدف بالتخفي والنجاة،كما يجب وضع خطة محكمة لاماكن تمترس السلاح والمعدات تتمشى مع طبيعة الأرض الكائن عليها،كما تمنع أي تحركات أو إشارات غير ضرورية داخل الموقع،وقد دللت تجارب القتال على أنه من السهل رؤية الهدف المغاير للطبيعة من خلال السكون أو الحركة، لذا فإن إمكانية تدميره سهلة ومؤكدة، أما الهدف المندمج مع الطبيعة فإن من الصعب كشفه وخاصة خلال السكون، كما أن إصابته تكون صعبة حتى بعد كشفه.

تحتوي منظومة الدفاع الجوي على مكونات عديدة مختلفة، مثل رادارات الإنذار ورادارات إدارة النيران، ورادارات التوجيه، ووسائل التوجيه التلفزيوني والحراري، ومراكز تحليل ونشر المعلومات، بالإضافة إلى سلاح المدفعية م/ط والصواريخ د/جو كأهم عناصر للنيران في الدفاع الجوي،وتعاني وسائل إنذار الدفاع الجوي بشدة من كثافة الأعمال الإلكترونية المضادة، ويرتكز جزء كبير من التطور التكنولوجي لتلك الوسائل في اتجاه التغلب على الإعاقة الإلكترونية وذلك بالخداع بطمس حقيقة المواصفات الفنية لوسائل الإنذار، حتى لا يتمكن العدو من وضع برنامج الإعاقة المناسب أو يضع البرنامج الخاطئ موضع التنفيذ، وبذلك يقلّ تأثير تلك الإعاقة، كما أن جميع الرادارات الحديثة تعمل بالأساليب الرقمية، التي من خلالها يمكن استبعاد إشارات الإعاقة أو التقليل من آثارها.

يخدم الخداع و التمويه سلاح الدفاع الجوي عن طريق أخفاء وتمويه القطع القتالية الأصلية أو استخدام قطع قتالية وهمية، وهو عمل إحترافي تقني هدفه

خدمة الخطة الدفاعية، لذا فإنه لا ينفذ إلا بناءً على أوامـر وتوجيهـات القيـادة العملياتيـة للدفاع الجوي حتى لا تتعارض نتائج المبادرات الخداعية الفردية التـي قـد يقـوم بهـا قـادة الكتائب أو قادة الألوية مع الأساس العملياتي لخطة مناورة قائد القوه، ومع الدور التكتـيكي لخطة الخداع والتمويه للدفاع الجـوي، وحتـى لا تتعـارض في النهايـة مـع خطـة العمليـات الاستراتيجية على المستوى العملياتي العام، ويعتبر التدبير الخـداعي الوحيـد المـتروك لمبـادرة قادة الوحدات التكتيكية هو الخداع المحـدود بأسـلحة متفرقـة، والخـداع بتمويـه وتـشويه بعض الأهداف لغرض حمايتها فقط.

أساليب ووسائل التمويه والخداع في العمليات العامة

أولاً وسائل التمويه والإخفاء:

عند البدء بعملية التمويه والإخفاء لا بد من إتباع مجموعة من الخطوات الرئيسية للتنفيـذ وتبدأ الخطوة الأولى للتمويه بدراسة طبيعة الأرض المحيطة بالموقع ونوعية تضاريسها، مـن حيث دراسـة ألوانهـا الغالبـة ومـدى قـدرتها عـلى عكـس الأشـعة وحجـم الظـلال المنتـشرة فيهـا وإمكانيـة انطبـاع الآثـار عليهـا، ويـلي ذلـك دراسـة نـوع التمويـه المطلـوب، حـسب بعد العدو وقربه، والأجهزة التي يستخدمها في رصده وكلما ابتعدنا عن العدو قلّـت أهميـة التمويـه ضـد الرصـد الأرضي، وكلـما انخفـض مـستوى الأجهـزة التقنيـة التـي يـستخدمها رصده الجوي أو الالكتروني قلت أهمية التـدابير المتخـذة لمجابهـة الأجهـزة المتطـورة، وتـأتي بعد ذلك الخطوة الثالثة المتمثلة في تحديد طبيعـة الهـدف ذاتـه، والعوامـل التـي تكـشفه للرصـد الجـوي: اللـون والـشكل واللمعـان و الظـل و القـرائن الدالـة، وتتمثـل الخطـوة

الرابعة في العمل على إخفاء هذه العوامل حتى يتم اندماج الهدف مع الطبيعة إلى أكبر حد ممكن، أما المرحلة الخامسة فهي إبقاء التمويه مادام الخطر مستمراً.

يعرف التمويه: بأنه مجمل العمليات التي تستهدف إخفاء القوات والمعدات والوسائط الصديقة عن الرصد المعادي بكل أنواعه، كما أنه مجموع الإجراءات التي تتخذها الأفراد أو القوات للاختفاء عن رصد العدو البري والجوي بكل أشكاله البصري والتصويري والالكتروني، دون أن يعيق هذا الاختفاء المهمة القتالية، كما أن التمويه سلاح دفاعي سلبي، يعتمد على إخفاء الهدف وسط المعالم على مبدأ الاندماج مع الطبيعية المحيطة به، كما أن كل إجراء يؤمن الاختفاء على حساب وقت وزمن تنفيذ المهمة القتالية لا يمكن أن يعتبر تمويهاً لأنه يعرقل ويؤخر القوات المسلحة من القيام بتنفيذ المهمة المنوطة بها،كما يفقد التمويه جدواه إذا لم يكن إحترازياً ولم تراع السرية في تنفيذه كما تراعى سرعة الانتشار كونه يفقد الهدف بعض ملامحه،ويمكن اعتبار التمويه نظاماً لإدارة البصمات، إذ إن القوات لا بد من حمايتها ضد الاكتشاف والتمييز والهجوم، حتى وهي متحركة وتشمل إدارة البصمات جميع الإجراءات السلبية الممكن اتخاذها في النطاق الكهرومغناطيسي، وتشمل التصميم الإنشائي واستخدام المواد الخفية وتقنيات الإخفاء.

ولكي يكون التمويه فعالاً ينبغي أن يؤمن العناصر التالية:

لزوم الاختفاء عن المراقبة الأرضية، ضرورة الاختفاء عن المراقبة الجوية بما في ذلك محاولة تجنب الصور الجوية العادية و الملونة، الاختفاء عن أجهزة

الرصد التي تكشف الحرارة والرائحة وصوت حركة الجنود أو سلاسل الآليات، أن يتم في كل ظروف المعركة وفي الليل والنهار مهما كان العدو بعيدا،ضرورة أن يكون الإخفاء مستمراً،أن يتأصل في نفس المقاتلين حتى يصبح غريزياً، أن يتم بإبداع وابتكار مستمرين.

المبادئ الأساسية للتمويه :

1- اختيار الموقع:

يتم اختيار الموقع حسب طبيعة الأرض سواء كانت صحراوية أو زراعية أو غابات كثيفة وعند اختيار الموقع واحتلاله يجب أن يبدو وكأنة لم يتغير بسب وجود الأفراد والمعدات ويجب ألا يعيق الموقع الذي وقع علية الاختيار أنجاز المهمة ويجب إنشاء انتخاب الموقع تجنب العلامات الأرضية المعزولة مثل الأشجار والنباتات.كما يتم اختيار الموقع حسب نوعية السلاح والأفراد فمثلا في الدفاع الجوي يراعى في اختيار أو احتلال الموقع ملائمته لتمويه وإخفاء الأسلحة والمعدات فمنظومة الصواريخ د/جو عند احتلال مواقعها لابد أن يكون الموقع يتلاءم مع احتياجات التمويه والإخفاء وكما هو الحال مع منظومة القيادة والسيطرة ومنظومة المدفعية م/ط.

شروط الموقع الأساسية التي لا بد من توفرها عند اختياره وهي:

- لا بد أن يوفر إخفاء كامل للمعدات والأفراد عن نظر العدو بالإضافة إلى الحماية والتمترس من نيران العدو وذلك حسب نوع الأسلحة.

- موقع يسمح بالحركة بمرونة أثناء الضرب والمناورة في القتال (الانسحاب، التقدم، تغير المكان).

- أن يتمتع بحماية كاملة ضد الهجمات المباغتة من مشاة العدو على الأرض من الأمام والخلف واليمين واليسار.

- أن لا يعيق الضرب أو الإطلاق من أيً من الأسلحة داخلة على حساب الآخر أي يسمح للجميع بالمشاركة.

- أن يسمح بكثافة الضرب أو الإطلاق والسيطرة على سير المعركة.

2- نظام التمويه :

وينقسم نظام التمويه والإخفاء إلى قسمين هما التمويه النهاري والتمويه الليلي، وتعتبر عمليات التمويه والإخفاء النهاري من الضرورة في الدرجة الأولى حيث يجب استعمال الممرات والطرق الطبيعية مع ملاحظة أي تغيير فيها مهما كان نوعها بل يجب إتباع قواعد التمويه وإتباع قواعد التحركات من وإلى المواقع لأن الحركة من أهم عوامل الانتباه والعين سريعة في التقاط أو ملاحظة أي تحركات كما أن التصوير الجوي يستطيع إيضاح أي شيء قد تحرك حتى في ظلام الليل باستخدام الكشاف أما في النهار فأنه ظاهر بطبيعة الحال، أن عملية التمويه والإخفاء الليلي أقل ضرورة من النهار ولذلك نستطيع الاستفادة من الظلام لمنفعتك وهو ذو منفعة مزدوجة للابتعاد عن جلب الانتباه ويجب ملاحظة أن الصور التي تؤخذ من الجو في الليل بواسطة طلقات الإشارة فهي تظهر العيوب الموجودة في الموقع من تحركات ونظام الأنوار في الليل مهم

وكذلك الأصوات لان الصوت في الليل يسري أكثر منه في النهار، وكذلك يجب التقليل من نداء الأفراد بعضهم لبعض حتى بالهمس إلا إذا اقتضت الضرورة كذلك هو الحال مع الأنوار بحيث تستعمل في أماكن لا يمكن ملاحظتها كداخل الخيمة والملاحظ أن العين ستقود إلى الرؤيا كل ثلاثين ثانية وعند إشعال ضوء تحتاج لنفس المدة للتعود على الإضاءة.

يعرف نظام التمويه بأنة عبارة عن تجنب كل مظاهر الأشكال والمعالم التي تعبر عن مظهر الموقع أو كشف أي هدف فيه والتي يمكن من خلالها أن يكشفها العدو وهي : الظل،اللمعان،اللون،الخلفية الضوئية،الصوت،الحركة،الآثار،الشكل الهندسي،الحرارة.

-الآثار الدالة على التمويه : وهي الدخان،الغبار، الضوء،الموجات التي تظهر بواسطة أجهزة الرصد.

3- الوسائل المستخدمة في عمليات التمويه والإخفاء:

عند تنفيذ عمليات الإخفاء والتمويه يراعى في ذلك استخدام المواد الصناعية والطبيعية للمساعدة العملياتية لدمج أشكال الأفراد والمعدات بطبيعة شكل الأرض المحيطة والكائن عليها الموقع، والمواد الصناعية هي تلك المواد الخاصة لعمليات الاختفاء والتمويه من الدهانات والأسلاك والخيش والأسلاك الشائكة والنسيج والشبكات المزخرفة وغيرها، والمواد الطبيعية هي المواد الطبيعية المحيطة أمثال الحشائش والأشجار والمياه...الخ وهذه المواد إذا أحسن اختيارها فأنها ستضاهي نماذج طبيعة الأرض المحيطة بالشكل واللون وهناك

سبب واحد وهو أن النباتات تذبل وتبهت إذا قطفت وتلافياً لذلك يتم تغييرها بسرعة.

ثانياً وسائل الخداع:

عرف الخداع على أنة عكس التمويه حيث يهدف التمويـه إلى إخفـاء المواقـع بيـنما يهـدف الخداع إلى كشف المواقع أو بعـض القـوى والوسـائط المزيّفـة أو المموهـة، وإعطـاؤه شـكل الهدف الحقيقي، أو تشويه الهدف الحقيقي الذي يصعب إخفاؤه بحيث يبدو وكأنه هدف مدني أو عسكري مدمر، أو هدف عسكري أكبر أو أصغر من حقيقته.

أنواع الخداع :

أ/الخداع البصري:

يمكن أن تنخدع عين الإنسان من خلال تأثير خـداع مـن بعـض الإجـراءات العاديـة كالـضوء والألـوان والعلامـات وغيرهـا، مـن هنـا دخلـت هـذه الإجـراءات الـسابقة عـلى الـصور أو المعالم المميزة عـلى المركبـات والأسـلحة، كـما أن اختيـار المواقـع المناسـبة قـد يـساعد أيـضا في عملية الخداع البصري مثلا خلـف البنايـات أو الأشـجار، إلا أن الأهـداف تـشكل سلـسلة من البـصمات أو المـؤشرات التـي قـد تكـون بـصرية أو الكترونيـة أو سـمعية أو حراريـة أو مجموعة من هذه، فيمكن بواسطة التصوير الحراري اكتشاف الحرارة الصادرة مـن الهـدف من خلال الأشجار وشـباك التمويـه التقليديـة والـدخان ولـكي يكـون هنـاك تمويـه فعـال لا بـد مـن اسـتبعاد هـذه البـصمات أو تخفيـضها،ويمكن بـذلك اعتبـار التمويـه نظامـاً

لإدارة البصمات، إذ إن القوات لا بد من حمايتها ضـد الاكتـشاف والتمييـز والهجـوم، حتـى وهي متحركة. وتشمل إدارة البصمات جميع الإجراءات السلبية الممكن اتخاذها في النطـاق الكهرومغناطيسي، وتشمل: التـصميم الإنـشائي واسـتخدام المـواد الخفيـة وتقنيـات الإخفـاء ويتمثل في خداع وسائل التـصوير الفوتـوغرافي والتليفزيـوني، والـذي يمكـن تحقيقـه بإتقـان الإخفاء والتمويه للمواقع، والمعدات، والأهداف الحيوية، باستخدام شـباك التمويـه، خاصـة الأنواع الحديثة منها، والتي تخفي الطاقـة الحراريـة للمعـدات Infra Red Camouflage، وتقلل منها، بحيث لا تظهر في أفلام الأشعة تحت الحمراء، كما تعمـل بعـض أنـواع الـشباك الحديثة، على تشتيت الموجات الرادارية، التي تصدرها محطات وأجهزة الاستطلاع الراداري، فلا تنعكس من المعدات المخفاة أي انعكاسات رادارية، ويعرف هذا النوع بشباك التـشتت الراداري Radar Scattering Principles كما تعتبر أنواع الطلاء الحديثة، من الأنواع، التـي تستخدم في تكنولوجيا الإخفاء، من الوسائل الحديثة في الإخفاء الراداري.

ب/خداع التحركات:

ويتم عـن طريـق خطـة متكاملـة، لتبـادل احـتلال المواقـع بالمعـدات الحقيقيـة والهيكليـة، مـــع الأخـــذ في الاعتبـــار، إتقـــان إخفـــاء المعـــدات الحقيقيـــة، وإظهـــار الزائفـــة بـصورة الحقيقيـة فبالتـدريب والـوعي للأفـراد ومـن خـلال بـذلهم جهـود هائلـة مـن التحركات لاحتلال ونشر منصات الصواريخ وتوزيع الطـائرات الاعتراضيـة التـي الكثـير منهـا زائـــف لإخفـــاء التحركـــات الحقيقيـــة وعـــلى القـــوات التـــي تريـــد النجـــاح لخطتهـــا الخداعيـــة في إخفـــاء حقيقـــي وإظهـــار الزائـــف بـــصورة الحقيقـــي الـــسعي إلى

خداع محللو بيانات استطلاع العدو.ومن أبرز الأمثلة خداع التحركات، الذي نفذته القوات المصرية، في حرب الاستنزاف، وما قبل العبور عام 1973، فلم يعرف الإسرائيليون، أين ومتي سيكون العبور، بالرغم من ظهور معدات وكباري العبور بالقرب من قناة السويس إيذاناً بقربه.

تعمل إحدى الشركات السويدية على إنتاج شراك خادع للتحركات متينة وقابلة للنقل وسهلة التركيب لجميع المعدات العسكرية، كما أنها مجهزة بكل ما يلزم من بصمات بصرية وحرارية ورادارية، ويتميز كل من هذه الشراك بغطاء ناعم فوق هيكل بنيوي متكامل مع البصمات المطلوبة، وتراعي الشركة المصنعة أهمية أن تكون الشراك قادرة على مقاومة الأحوال الجوية القاسية، وأن تكون قادرة على امتصاص واستيعاب الإصابات المتعددة بدون أن تنهار أو تضعف.

ج/خداع المواقع:

يتم تنفيذ عمليات خداع المواقع من خلال تصميم مواقع دفاع جوي هيكلية خداعية متعددة تقوم باستنزاف جزء كبير من إمكانات هذه التهديدات، علاوة على تقليل احتمالية إصابة الرادارات الأصلية أو إعاقتها الكترونياً، وتزود مواقع الدفاع الجوي بوسائل الخداع الإيجابية مثل مشبهات الرادارات التي تعمل على إرسال إشعاعها بترددات مقاربة للرادارات الحقيقية وبنفس مواصفات التعديل سواء كانت من هوائي مثبت وأصغر من الهوائي الأصلي، مع إمكانية محاكاة وتقليد دوران هوائي الرادار الأصلي بطريقة عمل إلكترونية، ويمكن للمواقع الخداعية أن تكون موجودة بالقرب من المواقع الأصلية، ويمكن أن تزود أيضاً بوسائل الخداع السلبي ووسائل الاستطلاع والقصف المحمولة جوا سواء الرادارية

أو التلفزيونية أو التي تستخدم الأشعة تحت الحمراء، من خلال إنشاء مواقع خداعية تحاكي الموقع الأصلية والتي تمثل نفس مكوناتها ومعداتها، بحيث تصنع نماذج هذه المعدات مطابقة للحجم الطبيعي للمعدات الأصلية بحيث تكون مواد البناء والتصميم قليلة التكاليف مع إضافة بواعث إيحاء لأشعة الكشف تحت الحمراء مع مراعاة محاكاة الموقع الأصلي من الناحية الإدارية والاتصالات السلكية واللاسلكية.

قامت إحدى الشركات في المملكة المتحدة بإنتاج أهداف وهمية قابلة للنفخ، تشمل الدبابات T-62 وT-72 وناقلات الجنود المدرعة BMP-1وBTR-60PB، وتم تطويرها لتحقيق التدريب الواقعي للمراقبين الجويين الأماميين وهم يوجهون طائرات الهجوم الأرضي ضد المركبات القتالية المدرعة وغيرها من تشكيلات ميدان القتال، وهي تستخدم في تلك المهام من قبل سلاح الجو الملكي البريطاني، كما يمكن استخدم نفس التقنيات لإنتاج أهداف خادعة للمركبات القتالية المدرعة والطائرات التابعة للقوات الصديقة، وفي حال النظر إلى تلك الأهداف من خلال المناظير العادية يمكن تمييزها كمركبات مدرعة على مديات تصل إلى 2-3كم، أما على مديات 900 - 1000م فيمكن تمييزها من حيث النوع، في حين يمكن تمييزها كأهداف وهمية فقط على مدى يقل عن 300م، وتصنع تلك الأهداف من النايلون المغطى بالمطاط، وهي تتكون من إطار من أنابيب قابلة للنفخ مغطاة لتشبه المحيط الخارجي للمركبة، أما المعالم البارزة كالعجلات والفتحات فإنها تطلى على القماش، وهناك دعامات وشدادات لعمل التوازن، ويشمل التصميم صمامات لضبط ضغط

الهواء أثناء النفخ أو عند ارتفاع درجات الحرارة، وتتم عملية النفخ بواسطة منفاخ صغير يعمل بطاقة البطارية، ويتم انجاز مهمة النفخ خلال 8-5 دقائق، وتتطلب الأعمدة و الشدادات 3-2 دقائق إضافية لتحتل مواقعها، وهناك العديد من الأنابيب التي تساعد على سرعة تفريغ الهدف من الهواء، وعادة يمكن لشخصين تفريغه من الهواء وحزمه وتخزينه في غضون 10 دقائق، وكل هدف يحفظ في حقيبة لسهولة المناولة والتخزين.

د/الخداع الإلكتروني :

هو أحد أساليب الحرب الإلكترونية، ويعرف بأنه تعمُّد إرسال موجات كهرومغناطيسية، أو تغيير اتجاهها أو امتصاصها، أو انعكاسها، بغرض تضليل العدو. والخداع الإلكتروني يتم عن طريق التقليد، أو التضليل، أو تمثيل نشاط إلكتروني؛ فالخداع عن طريق التقليد هو إحداث خلل في جزء من شبكات العدو الإلكترونية عن طريق إشعاع موجات كهرومغناطيسية بنفس الأسلوب الذي يتبعه العدو والدخول بها في شبكاته بغرض إرباكه، وأهم أنواع الخداع الإلكتروني في الدفاع الجوي هي:

(1) إعاقة وسائل استطلاع العدو:

ويكون بخداع الموجات الرادارية لوسائل استطلاع العدو، وذلك عن طريق تغيير اتجاهها أو امتصاصها، وانعكاسها بصورة مختلفة، لا تعبر عن واقع الأهداف المنعكسة منها. حيث يمكن الدخول إلى شبكات إنذار العدو بالبث على موجاته وافتعال أهداف كاذبة وإشارات وهمية مما يكون له الأثر في وصول العدو إلى

استنتاجات خاطئة يبني عليها قراراته من خلال إرسال طائراته لتدمير هذه الأهداف، ويمكن الدخول إلى شبكات الإنذار المعادية، وبث أهداف كاذبة، وبيانات وهمية، مما يؤثر على قرارات واستنتاجات العدو.

(2) الإعاقة المضادة للإعاقة:

ويتم ذلك، عن طريق حماية المحطات الرادارية، ووسائل الاستطلاع من إعاقة العدو لها، بتغيير الترددات، بسرعة كبيرة، حتى لا يتمكن العدو من ملاحقتها، وباستخدام تكنولوجيا انتخاب الهدف المتحرك، وكذا تقليل الفصوص الجانبية.

(3) خداع الصواريخ الموجهة والقنابل الذكية:

تعتبر هذه الوسيلة آخر الوسائل بعد وصول طائرات العدو فوق مواقع القوات وإطلاقها الصواريخ، فالصواريخ الموجهة يمكن قفل المحطات وتوجيهها 180درجة فيستمر المتطور منها على آخر معلومه لديه فتكون فرصة إصابته خفيفة واستخدام العواكس الركنية بخداع الصواريخ المضادة للأشعة تحت الحمراء أما الصواريخ التلفزيونية فيمكن إطلاق قنابل دخان لإخفاء المواقع، أما التشويش السلبي فهو الإعاقة على رادار الطائرة بدون إرسال أي موجات مضادة ولكن هو عبارة عن أشكال معينة من المواد العاكسة للإشعاع وتكون لها مقاطع رادارية تكون مثل أشياء معينة مثل أربعة قطع من هذه الأشكال تمثل في المقطع الرادار عدد 2 قاذف بتشورا فتظهر على الرادار كأنها فعلا 2 قاذف بتشورا فيتم ضربها بدلاً من القواذف الحقيقية.

ثالثاً وسائل وتقنيات التشويش الخداعية :

التشويش أحد أنواع وسائل التمويه والخداع، والذي يعرف بأنه مجموعة من الإجراءات الرئيسية للحرب الإلكترونية، التي تهدف إلى المنع أو التقليل من استخدام المجال الكهرومغناطيسي الفعال المعادي، ويتم ذلك من خلال رفع مستوى إشارات التشويش الدفاعية لتكون أعلى من إشارات المرسلة من الجهاز المعادي بهدف حجب المعلومات عنه.

عادة ما يكون التشويش من هذا النوع ضجيج في مجال محدود بإرسال نبضات مستمرة على نفس تردد جهاز العدو لتضليله، ويتم ذلك بمعرفة مواصفات الجهاز الإلكتروني المعادي، من حيث قدرة الإرسال والاتجاه، وقد يكون التشويش في مجال عريض، وذلك في حالات التوتر الشديد، والهجوم خاصة، وفي حالة كشفه من قبل العدو، فإن هناك إجراءات مضادة يجب إتباعها، ومنها تغيير التردد، أو زيادة قدرة الإرسال، أو استخدام مصدر تشويش إضافي، فيصعب على العدو التعامل مع مصدرين في نفس الوقت. وهناك نوع ثالث من التشويش يطلق عليه (التشويش المكتسح) وهو يجمع بين صفتي التشويش الضيق المجال والعريض المجال، وتكون إشارة التشويش متحركة باتجاه واحد من أدنى تردد إلى أعلى تردد.

العواكس الركنية:

تستخدم العواكس الركنيـة لأغـراض الخـداع الـراداري في الـدفاع الجـوي عـن طريـق تمثيـل أهداف هيكلية ذات مقطع راداري يقترب من الأهداف الحقيقية، ويمكـن باسـتخدام هـذه العواكس بمثيل المدفعية ومواقع الصواريخ والأهداف الاخرى، والعـاكس الركنـي عبـارة عـن مجموعة من الأسطح المعدنية المتعامدة، بحيث يؤدي هذا التعامد إلى عكس أشعة الـرادار الساقطة عليها بكمية كبيرة، كأنها منعكسة من هدف حقيقي كبـير، وقـد تكـون العـواكس مثلثة الشكل أو مربعة أو دائرية، ويمكن وضع العواكس في الدائرية في كـرات مـن المطـاط لاستخدامها كشراك خداعية طافية فوق سـطح المـاء لخـداع الـصواريخ البحريـة. ويمكـن أن تحمل العواكس الركنية عوامـات خاصـة يـتم قطرهـا بواسـطة الـسفن لاصـطياد الـصواريخ المضادة للسفن أو أن تحمل على الطائرات الموجهة بدون طيار لاصطياد الـصواريخ المـضادة للطائرات.

وهناك العواكس الركنية الرادارية وهي معدات خاصة تتميز بـأن مواصـفات الإشـارة الراداريـة المنعكـسة منهـا والتـي تكـون محـددة سـلفا، وتـستخدم هـذه عـلى نطـاق واسـع في الإخفـاء الراداري، مثل إخفاء معالم الساحل أو حدود المسطحات المائيـة، أو ممـرات هبـوط الطـائرات، حيث تصبح الصورة مشوشة على شاشة الرادار ويصعب تمييز الأهداف، كما تستخدم العـواكس الركنية لعمل أهداف كاذبة بغرض خداع العدو مما يؤدي إلى ظهور أهداف كثـيرة عـلى شاشـة الرادار وزيادة تحميـل معـدات توجيـه النـيران وهـذا بـدوره يقلـل مـن فاعليـة نـيران العـدو،

حيث يقوم الهدف الكاذب بعمل مصيدة رادارية تجذب الصواريخ الموجهة إليه، فيقل بالتالي احتمال إصابة الهدف الحقيقي

الأشعة فوق البنفسجية (UV) :

إضافة إلى وسائل الكشف البصرية العادية يمكن أيضا للتصوير بواسطة الأشعة تحت الحمراء(IR) التقاط الضوء المنعكس في ما وراء نطاق الضوء البصري، ويمكن تطبيق هذه التقنية في مهام الاستطلاع ليلاً، وتشمل إدارة البصمات أيضا الحماية ضد جميع أنواع أجهزة الاستشعار الحرارية، بالإضافة إلى الحماية ضد أجهزة الرادار بما في ذلك أجهزة الرادار المليمترية المطبقة مع أنظمة التسديد في المراحل النهائية، وتشمل الأنظمة أيضا الإشعاع فوق البنفسجي (UV) وقد طورت إحدى الشركات الأمريكية نظام شبكة تمويه بالغة الخفة تسمى (ULCANS) تحل حالياً مكان نظام الحجاب التمويهي خفيف الوزن (LCSS)في خدمة الجيش الأمريكي، ونظام شبكة تمويه(ULCANS) وهو نظام دعم وتعزيز قابلية النجاة في مواجهة التهديدات متعددة النطاقات البصرية والرادارية و تهديد الأشعة تحت الحمراء، وذلك من خلال تحقيق خفض احتمال الاكتشاف البصري وتعزيز شدة الإشارات الحرارية والرادارية، وتحسين التوافق مع التضاريس الخلفية مقارنة بنظام(LCSS).

وكان نظام شبكة التمويه(ULCANS) الخاص بمناطق الأحراش والغابات قد دخل مرحلة الإنتاج في عام 1999، أما النموذج الخاص بالصحاري فقد دخل الإنتاج في عام 2001، أما النماذج الخاصة بالمدن والمناطق القطبية وتلك المعززة ضد الرادار والأشعة تحت الحمراء(IR) فقد طورت ونشرت في العامين

2002 و 2003،ولتحقيق الوقاية ضد الأشعة تحت الحمراء فإن الشبكة تعمل على تخفيض فقد الحرارة بما يفوق80 %، وهي أيضا تبرد وتسخن وفقاً للخلفية سواء كانت حشائش أو صحراء، ويعمل النظام على تخفيض الاكتشاف بواسطة أجهزة الرادار من خلال تصغير المقطع الراداري، ويزن نظام (ULCANS) بأكمله حوالي 8,40كجم، ويشمل حاجزاً سداسياً وآخر متوازي الأضلاع وجهاز إصلاح داخل صندوق قابل للحمل والنقل، أما نظام الإسناد الذي يتضمن أعمدة وأوتاداً وغيرها فهو أيضا داخل صندوق آخر خاص.

تكنولوجيا التمويه والتعمية والخداع

أولاً: تكنولوجيا التمويه

التمويه، هو عملية إخفاء الأهداف أو الأفراد عن الخصم، مما يجعلهم يبدون وكأنهم جزء من الخلفية الطبيعية. ومهما تطوَّرت تقنيات القتال على جميع الأصعدة؛ براً، أو بحراً، أو جواً، يبقى التمويه هو خط الدفاع الأجدى والأوفر للهدف "أفضل وسيلة للوقاية".

وهو كذلك إخفاء المعدات الإلكترونية عن الخصم بالاستفادة من الظواهر الطبيعية الموجودة في المنطقة، خاصة وأن غالبية المعدات أو هوائياتها تكشف عن نفسها، وتحتاج لجهود مضنية لإخفائها عن ملاحظة الخصم.

1. تكنولوجيا التمويه اللاسلكي

تزايد استخدام الاتصالات في الحروب الحديثة على كافة المستويات، وأصبح لها دور فعّال في توجيه العمليات واستمرارها؛ إذ تمثل العصب الرئيسي في

إدارة أي صراع مسلح، وتبعاً لذلك أصبحت أحد الأعمال الرئيسية للقوات المتحاربة، مراقبة إرسال الخصم، ومحاولة التحكم فيه، واعتراضه، والتنصت عليه. وهناك عدة طرق لحرمان الخصم من إمكانية متابعة/ اعتراض التنصت على المواصلات الإشارية الصديقة، منها على سبيل المثال، التوقف الإرادي عن الإرسال "فرض الصمت اللاسلكي"، بهدف التضليل، أو استخدام أقل خرج لأجهزة الإرسال اللاسلكي، أو اللجوء إلى طريقة الإرسال بتقنية التردد القافز التي تعتمد على سرعة الإرسال العالية. ومن إيجابيات هذه التقنية أنها تقاوم عمليات التشويش الإلكتروني.

من جهة أخرى، تنخفض احتمالات النجاح في التنصت بشكل حاسم في حالة استخدام إجراءات التأمين الإلكتروني. كما يتبع، حالياً، مثل تثبيت هوائيات الإرسال والاستقبال في أماكن مرتفعة، ملائمة لساحة القتال، وبعيدة عن مراكز القيادة، إضافة إلى استخدام موجات الميكروويف التي يصعب اعتراضها من خلال التقنيات التقليدية.

2. تكنولوجيا التمويه ضد الصواريخ

هناك معدات تمويه للصواريخ، ويُشار إلى أن الصاروخ ذو التوجيه بالأشعة تحت الحمراء، يتأثر بدرجات متفاوتة بالسحب، مثل نوعيات الدخان التي تطلقها الطائرات. وفي الوقت الحالي، تطوِّر عدة شركات خرطوشات تحمي الطائرات العمودية من خلال نشر غيوم من الرذاذ "الإيروسولات"، مما يشكل غشاوة/ سحابة فاعلة ضد الأنظمة الليزرية، وتحت الحمراء، وبعض الأنظمة

الرادارية. كما تستخدم المشاعل الحرارية لخداع أنظمة التتبع الباحثة عن الحرارة Heat Seeker.

ومع التقدم الذي طرأ على الصواريخ، وقدرات التمييز فيها تتركز الجهود، حالياً، على تطوير وحدات خداعية سهلة الإلقاء ـ كانت تعمل لفترة محدودة ـ لكن للنماذج المتطورة منها فترة عمل غير محدودة باستخدام أجهزة متطورة في الطائرة للتحليل المتطور؛ للإشعاع الصادر عن الصاروخ المهاجم، ومن ثم إطلاق الوحدات الخداعية في اتجاهه في الوقت المناسب؛ لينجذب إليها الصاروخ، مثل استخدام الرقائق المعدنية ضد الصواريخ الموجهة رادارياً، والمشاعل الحرارية ضد الصواريخ الموجهة حرارياً.

ونظراً لظهور الحاجة أحياناً إلى الحماية من الصواريخ المهاجمة من الأمام؛ سواء أُطلقت من البر، أو من الجو، فتتزايد الجهود حالياً لتطوير وحدات خادعة مدفوعة "منطلقة" صاروخية تستطيع الطيران أمام الطائرة.

3. تكنولوجيا التمويه الراداري

كانت البحرية الأمريكيّة أول جهة طورت وحدات تشويش رادارية صغيرة نشطة في نهاية السبعينيات من القرن العشرين الميلادي. وخلال حرب الخليج الثانية استخدمت طائرات البحرية الأمريكية الطائرات الموجهة من دون طيار، الكبيرة الحجم "براترويك"، للتمويه عن هدف راداري معادي. وقد جرى، مؤخراً، في الولايات المتحدة الأمريكية التعاقد مع شركة "ساندرز" SANDARS لتطوير جهاز تشويش من الجيل الثالث لصالح البحرية الأمريكية، ويطلق عليه اسم

"ستراب"، ومن الشركات الأخرى الناشطة في مجال الخادعات المقطورة ـ أهداف رادارية محمولةـ شركتا "ساب" SAP و"ماركوني" MARCONE لأنظمة المعدات الدفاعية. وأنتجت هذه الأخيرة خادعاً مقطوراً تجره الطائرة، استخدم بنجاح على متن طائرات "نمرود" NIMROD الإنجليزية، خلال حرب الخليج الثانية في 1991.

كانت أنظمة التشويش المحمولة على متن الطائرات المقاتلة موجهة/ مخصصة، في بادئ الأمر، نحو أجهزة الرادار المعادية "الإعاقة على الرادارات المعادية"، لكنها باتت موجهة/ مخصصة، كذلك، نحو الأجهزة الليزرية والعاملة بالأشعة تحت الحمراء. ولا يزال حاضن/ مستودع "وستنجهاوس" Westinghouse من نوع ALO-119 أكثر حاضنات التشويش الراداري انتشاراً في العالم، ويستخدم على نطاق واسع على متن طائرات F-16 الأمريكية، وتُعَدّ شركة "ماركوني" لأنظمة الدفاع في بريطانيا أهم منتج بريطاني لأجهزة التشويش الراداري؛ إذ طورت حاضن/ مستودع "سكاي شادو" Sky Shadow الذي يحمل/ يركب على طائرات هوك HOK، وتتعاون الشركة مع شركة نورثروب NORTHRUP على إنتاج نظام التشويش الراداري "زوس" ZOS المخصص لطائرات هارير Harrier.

4. تكنولوجيا التمويه بالطلاء

كان تمويه الطائرات أكثر عمليات التمويه صعوبة؛ سواء من ناحية اختيار اللون المناسب، أو مستوى اللمعان، وأهمية عدم البهر من الضوء المنعكس على الهيكل، وضرورة محاولة خفض هذه المتغيرات من على السطح وإلى الحد

الأدنى الممكن، وأهمية جعل ألوان إشارة السلاح الجوي غير زاهية لعدم كشف الخصم لها.

وإضافة إلى ما تقدم، فإن فاعلية تكنولوجيا التمويه بالطلاء قد تفسدها أجهزة مختلفة مستخدمة في الطائرة لتسهيل الصيانة، إلا أنه في محاولة لتحسين تمويه طائرة فانتوم تابعة لسلاح الجو الملكي البريطاني، جرى تخفيض عدد الإشارات الخارجية، كالاسم والدوائر وغيرها من 700 إشارة إلى مائة ونيف. ومن جهة أخرى، فمن الصعوبة بمكان إخفاء شكل قمرة القيادة، الذي يبدو من بعيد، كأنه فتحة سوداء تشير بوضوح إلى "قلب" الطائرة، إلا أنه يمكن تخفيض مستوى وضوح قمرة/ كابينة القيادة من طريق عدم استخدام الألوان الزاهية، وخوذات الطيارين الملساء ذات القدرة الكبيرة على عكس الضوء.

هناك طريقة مستخدمة كثيراً في التمويه، وتكمن في طلاء أجزاء الهيكل المخفية نسبياً بلون أفتح قليلاً من الأجزاء المعرضة، كالأسطح العليا للجناح والهيكل، وطلائها باللون نفسه، ولكن الداكن نسبياً. ويُعتقد أن هذه الطريقة في تغيير نسبة وضوح اللون، حسب وضع المسطح، ابتكرها سلاح الجو الألماني في الحرب العالمية الثانية. ولكن المثال الأوضح لتأثيرها يتضح، بجلاء، في ألوان طائرة F-16 التابعة لسلاح الجو الأمريكي. ومع ذلك، يؤكد بعض خبراء التمويه أن استخدام تدرج الألوان لا يؤثر بفاعلية، إلا إذا كانت الطائرة تسير في خط مستقيم، وعلى مستوى طيران ثابت، وحين تنحرف أو تأخذ في الدوران، فإن تأثير تدرج الألوان ينعدم، وقد ينعكس ذلك سلباً على وضوح الهدف.

5. تكنولوجيا التمويه باستخدام الألوان المتدرجة

إضافة إلى جعل عملية كشف الطائرة أكثر صعوبة، فإن التمويه قد يستخدم، كذلك، لإرباك الخصم فور اكتشاف الأهداف، ويمكن استخدام نمط من الألوان المتدرجة "لتمييع" شكل الطائرة، ومن ثم، جعل تحديد هوية الهدف أكثر صعوبة، واليوم أخذت عادة طلاء سطح الطائرة باللون الغامق، والسطح الأسفل باللون الفاتح، تتراجع أمام اللون الموحد لجعل الطائرة أقل وضوحاً حين ترصد من بعيد؛ سواء كانت مقبلة على الخصم أو مبتعدة عنه.

وقد أسهم الفنان الأمريكي "كيت فيريس" مع مدرب الطيران بسلاح البحرية الأمريكية، "سي ج هيتر هيتلى" في تطوير طريقة لطلاء المقاتلات عرفت باسميهما، وتتميز بأربعة خطوط متموجة، تراوح ألوانها بين اللون الأزرق الرمادي والرمادي؛ إذ يكمن المبدأ من وراء استخدام هذه الطريقة في أن ربع هيكل الطائرة، تقريباً، يختفي في أي محيط، مما يترك جزئين صغيرين منه لا يمكن تحديد هويتهما بسهولة، ومع ذلك فلم يقبل سلاح البحرية الأمريكية باستخدام هذه الطريقة في الطلاء، على أساس أن تكلفة إعادة طلاء مجمل مقاتلاته لم تكن مبررة.

6. تكنولوجيا التمويه باستخدام الطلاء المطفي اللمعة

جاءت طريقة الطلاء المعتمدة، والمستخدمة حالياً، مؤلفة من ثلاثة ظلال للون الرمادي، واختبرت طريقة التمويه الجديدة على طائرات F-4 لسلاح الجو في كل من بريطانيا وألمانيا في 1979، ثم طُلِّيت، فيما بعد، بالطلاء ذاته طائرات

TORNADO، وHAWK، وLIGHTNING، وجميعها تستخدم في بريطانيا في مجال الدفاع المنخفض عن المطارات. ومع ذلك، ونظراً لصعوبة المحافظة على أي طلاء نظيفاً، فقد فضل سلاح الطيران هذا الطلاء المطفي اللمعة، على الرغم من أنه قد يكون أقل فاعلية لجهة التمويه.

أدخل الطلاء المطفي اللمعة في سلاح الجو البريطاني بنهاية الثمانينيات من القرن العشرين الميلادي، وطُلِّيت به، للمرة الأولى، طائرة هارير GR-5 التي روعي في أن تكون الظلال عليها، بطلائين من "بوليوريتين الأخضر"، ونُفِذَّت التجارب باستخدام طائرتي هارير GR-5، وهوك، رسم على مقدمة هيكل كل منهما قمرة قيادة خادعة، إلاّ أن هذه الطريقة في الطلاء عُدّت خطرة جداً عند استخدام الطائرات في وقت السلم.

هناك خطوط تطوّر مختلفة في المؤسسة الملكية للجو والفضاء في "فارنبرة"، كما جرى تبادل المعلومات بين الولايات المتحدة الأمريكية وبريطانيا بخصوص الطلاءات الممتصة للإشعاعات الرادارية، التي لا تعمل سوى على نطاق ضيق من الترددات الرادارية، إلاّ إنها كانت مناسبة بدرجة كبيرة، ويعتقد أن مثل هذه الطلاءات استخدمت على طائرات لوكهيد LOCKHEED U-2 & SR71A، وهي مسحوق مغناطيسي مثبت بمادة مطاطية راتنجية Resin.

ثانياً: تكنولوجيا التعمية

هي خفض مسافة رؤية الهدف/ الطائرة إلى أقل وقت؛ بحيث يصعب على القوات المعادية التعامل معه. ولم يكن لوسائل التعمية، على امتداد الجزء

الأكبر من تاريخ الطيران، سوى تأثير محدود لحماية الطائرات، ولكن التطرق لهذا الموضوع أصبح ينفذ بشكل علمي بحت، خاصة في الولايات المتحدة الأمريكية وبريطانيا، وباتت طائرات التعمية المنتجة حديثاً، تخدع الراصد تماماً، ولا يمكن كشف حقيقتها؛ سواء بالنظر، أو الاستكشاف الحراري Infrared IR، وفي بعض الحالات لا يمكن تحديدها حتى بوساطة الرادار.

قديماً، بدأ اختيار أنواع متعددة من الطلاء، تولته قيادة الوحدات الجوية الملكية البريطانية المرابطة في مصر قبل اندلاع الحرب العالمية الأولى مباشرة، واعتمد أول طلائين للتعمية في العالم: الأول، اللون الرملي المائل إلى الاخضرار Standard Khaki أو PC-10 للاستخدام في أوروبا، والآخر، اللون البني الغامق المائل إلى الاحمرار PC-12 المستخدم في منطقة الشرق الأوسط.

1. هدف التعمية

إن هدف التعمية الأساسي في المفهوم الحديث هو خفض المسافة التي يمكن عندها رؤية الشيء بالعين المجردة، ويمكن تحقيق ذلك، بالدرجة الأولى، بالتخفيف من شدة وضوح الهدف بالنسبة إلى الخلفية المحيطة؛ سواء في الجو، أو البر، أو البحر، وذلك بالتحكم في لونه، أي تواتر انعكاس الضوء، ودرجة لمعانه، أي كمية الضوء المنعكس.

وتكمن الخطوة الأولى في اعتماد طريقة تعمية مناسبة في تحديد طبيعة الخلفية المحيطة بالطائرة. ويتوقف ذلك، بالطبع، على عمل الطائرة، فإما أن تكون

تعمل على ارتفاعات عالية، أو تكون طائرة على ارتفاعات منخفضة، إضافة إلى التهديد الرئيسي المتوقع، مثل نُظُم الدفاعات الأرضية، أو المقاتلات.

2. التعمية من طريق الأضواء الكاشفة المبهرة للعين

على مسافات بعيدة، عادة، تبدو الطائرات كنقاط سوداء ـ مهما كان لون طلائها ـ ولذلك فإنه يمكن خفض مدى الاكتشاف، نظرياً، بزيادة الإضاءة لإلغاء هذا التأثير البصري، وبنهاية الحرب العالمية الثانية بُذِّلت محاولات، في الولايات المتحدة الأمريكية وبريطانيا، في هذا المضمار باستخدام قاذفات قنابل مزودة بمجموعة من الأضواء الكاشفة المخصصة للهبوط، والمثبتة في مقدمتها وعلى الحواف المتقدمة للجناح، وكانت هذه الاستخدامات ناجحة بكل المقاييس، ولكن تنفيذ الأضواء القوية يتطلب طاقة كهربائية كبيرة ويصعب توفيرها بسهولة في الطائرات.

ظهرت بعض الأفكار بهدف تخفيض التباين بين الطائرة والخلفية المحيطة بها بقياس الشدة الضوئية في هذا المحيط، وإضاءة الهيكل؛ بحيث تتساوى الشدة الضوئية حوله مع الخلفية المحيطة به. وقد تستخدم مثل هذه الملائمة في الشدة الضوئية من أجل التمويه، نظرياً، حتى الآن على الأقل، في تمويه الطائرات الضاربة على مستويات منخفضة وقاذفات القنابل مثل TU-160 BLACK JACK. أما الغرب، فهو يتبنى تكتيك الاندفاع الخاطف على ارتفاعات منخفضة بطائرات مموهة لتعمية مستشعرات الكشف للرادارات المعادية.

3. تكنولوجيا التعمية المؤقتة باستخدام التمويه

هناك اتجاه نحو تطوير طلاءات التمويه المؤقتة المستخدمة في طائرات سلاح الجو البريطاني خارج أوروبا. وفي الماضي، كانت طائرات سلاح الجو البريطاني المنتشرة من أجل التدريب في شمال النرويج، إبّان الشتاء، تُطلى بطلاء أبيض ناصع، يُزال عند غسله بسهولة. وقد ثبت أنه يخفض من إمكان اكتشاف الهدف في محيط مكسو بالثلوج إلى جانب سهولة إزالته. ولكن هذا الطلاء، على الرغم من مميزاته، لم يستطع، في الواقع، مقاومة هذا الطقس، واضطرت إحدى الطائرات العمودية من نوع "بوما" PUMA إلى إلغاء إحدى الطلعات؛ نظراً لأن طلاء هيكلها، الذي جرفه الماء، غطى نافذة قمرة الطيار.

4. تكنولوجيا التمويه والتعمية في الشرق الأوسط

في نهاية الثمانينيات من القرن العشرين الميلادي طوِّرت مجموعة جديدة من طلاءات التمويه الجديدة في بريطانيا، وقد أُعطيت الأولوية لتمويه طائرات C-130، عند نشرها في منطقة الشرق الأوسط، وقد استخلص طلاء جديد، قلوي القاعدة، بعد إجراء تحاليل طيفية من أنواع الرمال في المنطقة، واختبر الطلاء في إحدى الطائرات C-130 المتمركزة في قبرص في 1988. وقد عُرِّف اللون الجديد، بصورة غير رسمية، بلون "النمر الأرجواني" Pink Panther، نسبة إلى الرسوم المتحركة الشهيرة لهذا الحيوان، وقد أصبح هذا اللون يعرف، الآن، رسمياً، بلون "رمال الصحراء".

عند حدوث أزمة الخليج، لم يكن هناك سوى القليل من هذا الطلاء، فطُلب على الفور المزيد منه من شركة "ترايمت المحدودة" TRIMITE للطلاء، لاستخدامه في طلاء طائرات سلاح الجو البريطاني المنتشرة في شبه الجزيرة العربية، وطوِّر إلى طلاء رمادي من السلسلة نفسها التي تستخدم في طائرات "جاجوار" JAGUAR، عند نشرها في شمال أوروبا.

ثالثاً: أعمال الخداع الإلكتروني ضد أسلحة القتال الحديثة الموجهة إلكترونياً

نظراً للتطور الهائل في مجال تكنولوجيا الإلكترونيات، واعتماد معظم أسلحة القتال، إن لم يكن جميعها، في أدائها لمهامها القتالية، على النظم الإلكترونية المتطورة، للقيادة، والسيطرة، والكشف، والتوجيه، والتحكم، سواء الأرضية، أو المحمولة بحراً، أو جواً. لذلك فقد تعاظم دور الخداع الإلكتروني، في التأثير بفاعلية على كفاءة هذه الأسلحة، في إصابة أهدافها، وبالتالي، تقليل نسبة الخسائر.

ومن هذا المنطلق، برز الخداع الإلكتروني بوصفه أحد العناصر الرئيسية الفعالة في مكونات إيجاد موقف إلكتروني وهمي، بصورة تخالف الواقع، باتخاذ بعض الإجراءات والأعمال؛ لتقليل درجة دقة المعلومات التي يمكن أن يحصل عليها الخصم بغرض تضليله وتشتيت جهوده، واستنزاف وسائله النيرانية، وذلك من أجل توفير الاستقرار المناسب للقوات، والوسائل الصديقة؛ لتحقيق مهامها القتالية بأقل خسائر ممكنة.

1. دور الخداع الإلكتروني ومكانه في منظومة الحرب الإلكترونية

يُعد من إجراءات الحرب الإلكترونية الدفاعية EW Defensive Measures، التي تنفذ لخداع وسائل العدو الإلكترونية المستخدمة في القيادة، والسيطرة، والكشف، والتوجيه، لقواته، وأسلحة قتاله، بتمثيل موقف إلكتروني وهمي للموقف الإلكتروني الحقيقي، أو بالتداخل على وسائله الإلكترونية، بغرض إرباكه، وتشتيت جهوده، واستنزاف وسائله النيرانية.

2. أساليب الخداع الإلكتروني

أ. تغيير/ تشويه المعالم الإلكترونية للأهداف الحقيقية.

ب. الإخفاء الإلكتروني الكامل/ الجزئي للأهداف الحقيقية.

ج. إيجاد الأهداف الإلكترونية الكاذبة.

3. حتمية الخداع الإلكتروني

نظراً لتكامل منظومتي الكشف، والتوجيه للمقذوفات بوسائلها الكهرومغناطيسية المتعددة، التي تتيح للعدو الحصول على معلومات تفصيلية ودقيقة عن الأهداف الحيوية وإصابتها، فقد استلزم ذلك ضرورة استخدام منظومة متكاملة للخداع الإلكتروني، يراعى فيها الحرفية، والواقعية، والحبكة، لتكون قادرة على خداع نظم الكشف والتوجيه المتعددة، مع الوضع في الحسبان، أن تكون هذه المنظومة قادرة على التعامل مع التهديدات الحالية والمستقبلية.

لا تُعد أعمال الخداع الإلكتروني أعمالاً هجومية، ولم تحظر، حتى الآن، في أي اتفاقيات دولية للحد من التسليح أو نزع السلاح.

تُعد تكنولوجيا الخداع الإلكتروني إحدى الضروريات، في ظل التفوق التكنولوجي للدول المتقدمة.

4. منظومة الخداع الإلكتروني المتكاملة عن الأهداف الحيوية

منظومة الخداع الإلكتروني المتكاملة: تنقسم في أساليب تنفيذها إلى الآتي:

أ. إخفاء الأهداف الحقيقية

وهي الأعمال الإلكترونية التي تتخذ بغرض تقليل احتمالات اكتشاف الأهداف الحقيقية، ومن أمثلة ذلك:

(1) شباك التمويه، وطلاءات التمويه والتعمية البصرية/ التليفزيونية، وأغطية الإخفاء الحراري، والراداري.

(2) الدخان ضد أنظمة الرؤية الضوئية والحرارية.

(3) سحابة الرقائق المعدنية ضد نظم الكشف الراداري.

ب. تشويه، معالم الأهداف الحقيقية أو تغييرها

هي الأعمال، التي تتخذ بغرض تغيير، المعالم، أو الشواهد الدالة للأهداف أو تشويهها، ومن أمثلة ذلك: استخدام العواكس الركنية لتغيير، وتشويه معالم

الأهداف، والشواهد رادارياً، واستخدام براميل المازوت المشتعلة، لتشويه الصورة الحرارية للأهداف.

ج. تمثيل أهداف كاذبة "نماذج هيكلية"

هي مجموعة الأعمال الإلكترونية التي تتخذ بغرض جذب انتباه أنظمة الكشف والتوجيه الإلكترونية إلى أهداف خداعية، وبالتالي، تقليل نسب الإصابة عن الأهداف الحقيقية، وزيادة نسب الإصابة للأهداف الخداعية، ومن أمثلة ذلك، الأهداف والنماذج الخداعية المطاطية "راداري، حراري، ليزري، تليفزيوني، بصري"، والعواكس الركنية "راداري"، والهيلوجراف Heliograph "ليزري"4.

د. الخداع اللاسلكي عن طريق التقليد

بإحداث خلل وإرباك في الشبكات، والاتجاهات اللاسلكية، وذلك بتقليد نوع العمل، أو الإشعاع، الذي ينبعث من أجهزة العدو اللاسلكية، والتداخل على قنوات مواصلاته بالأسلوب الذي يتبعه نفسه، باستخدام المحطات اللاسلكية الصديقة، وإرسال تعليمات خاطئة، وأوامر، وتقارير، وبلاغات قتال، وإشارات لاسلكية من خلالها، كأنها صادرة من العدو، بغرض إرباك قواته، وإفقاده السيطرة عليها.

5. كيفية تنفيذ الخداع اللاسلكي من طريق التقليد

تشغل المحطات اللاسلكية الصديقة؛ لتقليد عمل شبكات العدو اللاسلكية، بشكل مناظر لها تماماً، من طريق إرسال تعليمات خاطئة، (أوامر، تقارير، بلاغات قتال، إشارات لاسلكية) باسم العدو، بأسلوب سريع ومباشر، لخداع قادة هيئة القيادة المعادية وضباطها، إضافة إلى خداع عمال لاسلكي العدو، واضعين في الحسبان، السلوك الشخصي، والسمات المميزة لعمال التشغيل، وعلى الترددات، وأنواع العمل التي تعمل عليها الأجهزة اللاسلكية المعادية نفسها، حتى يتوهم هؤلاء العمال، أن هذه الإشارات صادرة من المحطات الصديقة للشبكات والاتجاهات اللاسلكية الخاصة بهم، مع مراعاة أن إرسال المعلومات الخاطئة، من خلاف الشبكات الصديقة، يجب أن تنفذ بطريقة لا تمكن العدو من اكتشافها، بحيث تأخذ في المظهر والشكل الأسلوب نفسه والطريقة المستخدمة في إرسال العدو للمعلومات الحقيقية له.

6. أعمال الخداع الصوتي Sonar Deception

يستخدم للحد من إمكانات الاستطلاع المعادي بالصوت "Sonar" في اكتشاف الغواصات، والسفن، والقطع البحرية الصديقة، وخداع نظم توجيه أسلحة القتال بالصوت ووسائله، وخاصة ضد الغواصات، ويشتمل على ما يلي:

أ. الستائر الغازية

تستخدم الستائر الغازية في تقليل انتشار الصوت، وتمثيل أهداف خداعية تحت الماء. وتتميز هذه الستائر الغازية بإمكان استعمالها في حدود مجال ترددي واسع.

تتكون من خراطيم خداع خاصة، عندما تلمس شحنتها الكيماوية الماء، يحدث اندفاع عنيف لفقاعات الغاز، وفي حالة اصطدام موجات أجهزة الكشف الصوتي "السونار" عن الغواصات بهذه الفقاعات، فإنها تعكس إشارات مشابهة لتلك المنعكسة من الغواصات.

باستخدام هذه الخراطيم الخداعية، يمكن للغواصة المناورة التخلص من القناصات، وعناصر مكافحة الغواصات المعادية التي تطاردها.

ب. الأغطية الهيدروصوتية

تستخدم لتقليل مدى اكتشاف الخصم للغواصات الصديقة.

من الناحية العملية، وجد أن عملية تصميم أغطية هيدروصوتية ذات مجال ترددي واسع، ويمكنها تحمل درجات ضغط مياه البحر، ودرجات الحرارة المختلفة، تواجه صعوبات كبيرة.

ج. المقلدات الصوتية

تستخدم في تمثيل أهداف كاذبة بإنتاج أصوات مشابهة تماماً لأصوات محركات الغواصات تحت سطح الماء، لخداع نظم التوجيه الصوتي لأسلحة القتال ضد الغواصات ووسائله.

د. كيفية استخدام المرسلات الخداعية/ المقلدات ضد الصواريخ المضادة للإشعاع الراداري.

هـ. إجراءات الوقاية من الصواريخ الموجهة رادارياً، باستخدام إحدى طرق الإخفاء والخداع الراداري للأهداف الثابتة والمتحركة

(2) استخدام مواد طلاء ماصة الموجات الكهرومغناطيسية.

(2) استخدام مواد طلاء تتداخل مع الموجات الكهرومغناطيسية.

(3) الاستفادة من طبيعة الأرض في إخفاء الشواهد الرادارية للأهداف باستغلال السواتر الطبيعية.

(4) استخدام الشباك المعدنية، والأغطية الماصة للموجات الكهرومغناطيسية.

(5) استخدام الرقائق المعدنية في توفير الحماية الذاتية للأهداف الثابتة، والمتحركة.

7. إجراءات الوقاية من الصواريخ الموجهة حرارياً

أ. تقليل الانبعاث الحراري الصادر من المعدات باستخدام الشباك المبللة، أو إجراء بعض التعديلات الميكانيكية في الأجزاء المشعة حرارياً.

ب. استخدام طلاء خاص لتقليل الانبعاث الحراري.

ج. استخدام المشاعل الحرارية لجذب المقذوفات الموجهة حرارياً بعيداً عن أهدافها.

8. إجراءات الوقاية من الصواريخ الموجهة بالليزر

أ. وضع مصادر إضاءة ليزرية بالقرب من الأهداف تكون مشابهة في قدراتها لأشعة الليزر المعادية المرتدة من الهدف، والمستخدمة في إضاءته حتى يمكن خداع الصاروخ الموجه بالليزر.

ب. استخدام الدخان لتشتيت أشعة الليزر المستخدمة في التوجيه أو امتصاصها.

9. إجراءات الوقاية من الصواريخ الموجهة تليفزيونياً

أ. استخدام طرق الإخفاء التقليدية، لإخفاء المعدات، والأهداف الحيوية.

ب. استخدام عبوات الدخان في تعمية الكاميرات التليفزيونية المستخدمة في التوجيه.

ج. استخدام طلاء مشابه للخلفية المحيطة بالهدف.

الفصل الرابع

الحرب الألكترونية في مسرح العمليات العربي-الإسرائيلي

الصراع العربي الإسرائيلي والمواجهة

عرف العالم منذ القدم مجموعة مـن الأزمـات و الـصراعات الدوليـة ,حيـث لم تخلـو حقبـة تاريخية من الحروب، التي غذتها في كثير من الأحيان الأطماع الإستعمارية لـبعض الـدول، و أفرزتها أزمات دبلوماسية و إقتصادية و سياسية و إيديولوجيا أحيانا أخرى...

و تعد الحروب النقيض الحتمي للسلام و الأمـن، و وسـيلة لتنفيـذ سياسـة الـدول بواسـطة العنف و الاكراه، خاصة بعد فشل الوسائل الدبلوماسية و السلمية، بإعتبارهذه الأخيرة اليـة للتخفيف من شدة التوترات، و فض النزاعـات الحاصـلة بـين الاطـراف في الفـترات المتميـزة بالشك و الحذر.

إن الحرب بمفهومها التقليدي، قد عرف تطورا سريعا تزامنا مع التقدم الحاصل في الوسـائل و المعدات المـستخدمة في العمليـات العـسكرية، و لعـل أبـرز العوامـل المـساهمة في ذلـك التغير، ذاك التطور الهائل الذي جاءت به الثورة التكنولوجيا و المعلوماتية و بصورة لم يسبق لها مثيل.

و تتعدد أشكال الحروب و أنواعها و وسائلها، حيـث لم يعـد مفهـوم الحـرب مقتـصرا عـلى الحروب النظامية العسكرية التي تنشأ بين دولتين أو أكثر، بل أصبحنا أمام حـروب جديـدة كتلك التي تشنها منظمات ارهابية، إضافة الى الحروب الإعلامية و المعلوماتية، أي أن الدولة القومية لم تعد مهددة من طرف الدول فقط، بل قد يكون أمنها في خطر أمام بضعة أفـراد ينتمون الى عدة دول مختلفة .

و تعد الحرب الإلكترونية ظاهرة جديدة في العلاقات الدولية الراهنة, بإعتبارها ذلك الوجه السلبي لإستخدام التطبيقات التكنولوجيا و المعلوماتية، بل أضحت من بين المخاطر و التهديدات الأمنية الجديدة، والتي تتجاوز في تداعياتها و أبعادها الحدود السياسية و الجغرافيا للدول.

ومنه فالأمن بمفهومه الكلاسيكي، لم يعد قادرا عن التعبير بصدق عن كافة التحديات و التهديدات، التي اصبحت تلقي بظلالها و إشكالاتها على مستقبل الأمن القومي للدول.

في الاسبوع الاول من ابريل 2013، عاشت اسرائيل على إيقاع الاختراقات الإلكترونية، والتي شنها شباب ينتمون الى عدة بلدان منها المغرب و تونس و ليبيا و فلسطين و الأردن و باكستان و أمريكا...

فرغم البعد الجغرافي، إلا أن العالم الإفتراضي و الهدف المشترك قرب و وحد بين هؤلاء المجموعات التي من بينها مجموعة " أنونيموس"« Anonymous » و مجموعة أشباح المغربية، الفلاكة التونسية، موريتان هاكر تايم و غزة هاكر تايم....

حيث قامت هذه الجيوش الإلكترونية بإختراق العديد من المواقع الإلكترونية الإسرائيلية, من أبرزها : موقع الكنيست الإسرائيلي و وزارة الاستخبارات، و رئاسة الوزراء وموقع وزارة الأمن...، إضافة الى 20000 حساب الفايسبوك و3000 حساب مصرفي في مختلف البنوك الإسرائلية.

و قد يعتبر البعض ان هذه الحرب الجديدة المعلنة من هؤلاء القراصنة, لا تخرج عن إطـار الـلـهو و الهواية و البحث عن الـشهرة. في حـين أنهـا تحمـل في طياتهـا رسـائل ذات طـابع سياسي في غاية من الأهمية، سواء تلك الموجهة لإسرائيل باعتبارها هدفا رئيسيا لهـا, أو تلـك الموجهة لدول العالم العربي الاسلامي خاصة و للمجتمع الدولي عامة.

حيث شكلت هذه الحرب الإلكترونية ,التي لا تقل في خطورتها و تداعياتها من التهديـدات العسكرية التقليديـة، مناسـبة للقـائمين بهـا في تجديـد رفـضهم التـام و المطلـق للانتهاكـات الجسيمة لحقوق الشعب الفلسطيني، وسياسة إزدواجية المعايير التي يتبناها مجلس الأمـن الدولي في الصراع العربي / الإسرائيلي.

فاختراق العديد من المواقع الرسمية لإسرائيل، هو بمثابة رسالة تحذيرية لهذه الاخيرة لعلها تعيد النظر في سياستها التوسعية و الوحشية التي تمارسها ضد إرادة الشعب الفلـسطيني، و الغير أخذة بعين الإعتبار لقواعد القانون الدولي الإنساني.

كما تعد هذه الحرب الإلكترونية التي قامت بها مجموعة الهـاكرز، محطـة لتـذكير في عـدم جدوى السلاح النووي لمواجهة هذه الأنواع من الحـروب، ويكمـن ذلـك في غيـاب إمكانيـة الردع في مثل هذه الحالات، بسبب كون مصدر الهجوم افراد و جماعات تنتمـي الى العديـد من الدول، مما يصعب معه احتواء هذا التهديد و القضاء عليه.

إن تعطيل العديد من المواقع الاسرائيلية الرسمية و مواقع التواصل الاجتماعية، يجعل إسرائيل بما تمتلكه من قدرات نووية، و بما تتمتع به من تقدم في مجال المعلوماتية و التكنولوجيا، في موقع ضعف أمام مواطنيها والعالم برمته, الذي من معالمه التشكيك في قدرتها – إسرائيل – على الحفاظ على أمنها المعلوماتي..

لقد ساهمت شبكة الاتصالات الدولية، المتمثلة في الانترنت في التقريب بين المنخرطين خلال عمليات الاختراق، عبر السرعة في تلقي المعلومة و توجيه الضربات بشكل فعال للهدف، ومنه تشكيل جيش إلكتروني يهدد الامن القومي الإسرائيلي في الصميم.

و اذا كانت الدول العربية قد عرفت حراكا اجتماعيا لم يسبق له مثيل، بفعل استغلال الشباب العربي لمواقع التواصل الإجتماعي، و الذي كان من نتائجه إسقاط انظمة سلطوية و إستبدادية و شمولية فقدت شرعيتها منذ زمن بعيد، فهو حراك تهيمن في اغلبه مطالب داخلية للشعوب العربية، كالمطالبة بالديمقراطية و الحرية و العيش الكريم و إحترام حقوق الإنسان... حيث لم يتم رفع شعارات ذات بعد خارجي مثل تحقيق الوحدة العربية أو تحرير فلسطين بإعتباره مطلبا قوميا.

فإستمرار الإحتلال الإسرائيلي للأراضي الفلسطينية، و تواطؤ العديد من الدول من بينها العربية مع الإحتلال، ساهم في خلق المزيد من السخط و عدم الرضى على السياسات الخارجية للدول العربية ازاء هذه القضية، والتي لا تستجيب لطموحات الشعوب. و منه فالأقطار العربية اصبحت مطالبة بإضفاء الشرعية

على سياساتها الخارجية، و عدم اتباع سياسة الإستبعاد و التهميش التي لا تتأتى و مبادئ الديمقراطية.

فمجموعة هذه الجيوش الإلكترونية قامت بدور و عمليات، عجزت الجيوش العربية و الإسلامية من تحقيقها على أرض الواقع أو على الأقل في العالم الافتراضي. حيث ألحقت بإسرائيل خسائر مالية و اقتصادية كبيرة ,التي كان من أسبابها تعطيل للخدمات التي تتيحها تلك المواقع الإلكترونية.وفرض حصار إلكتروني و عزلة عن العالم الخارجي.

فاذا كانت دول العالم العربي الإسلامي تبرر إخفاقها في إلحاق أضرار لسلطات الإحتلال الإسرائيلي، بكونها لا تتوفر على الإمكانيات و الوسائل لتحقيق ذلك الهدف، ففي عصر تغلب عليه شبكات الإتصالات الدولية، يصبح من المستحيل ممكنا عن طريق إستثمار ثمار التطبيقات المعلوماتية في هذا المجال.

و ختاما يمكن القول، أن تحقيق الأمن المعلوماتي لجميع الدول أصبح مطلبا ملحا في العقود الأخيرة، بفعل تنامي الحروب الإلكترونية التي تغذيها الثورة المعلوماتية، حيث لم يعد معها سيادة الدول حصنا منيعا للاحتماء من تحدياتها و مخاطرها و تداعياتها السياسية والاقتصادية.

رغم الأصداء الواسعة التي تركتها الهجمة الإلكترونية التي تعرضت لها إسرائيل مؤخراً والتي استهدفت مواقع وزارات ومرافق حكومية على الشبكة العنكبوتية، فإنه يمكن القول إن هذه الهجمة أبعد ما تكون عن الحرب الإلكترونية التي

تحسب لها النخب الحاكمة ودوائر التقدير الإستراتيجي في تل أبيب ألف حساب، وتعمل على مدار الساعة من أجل تحصين الكيان الصهيوني في مواجهتها.

إن ما يثير الذعر في إسرائيل هو أن تتعرض لهجمة إلكترونية تستهدف بشكل مباشر مرافقها الإستراتيجية المرتبطة بالفضاء الإلكتروني، مثل البنى التحتية (الكهرباء والمياه والمواصلات، والقطاع المصرفي..)، وهيئات القيادة وشبكات التحكم العسكرية، والأقمار الصناعية، وكذلك مجمل التقنيات المتقدمة المرتبطة بهذا الفضاء.

"سيناريوهات الرعب التي تخشاها إسرائيل من الهجمات الإلكترونية لا تكمن فقط في الشلل الذي يمكن أن يصيب الكيان الصهيوني, بل في سقوط عدد كبير من القتلى في صفوف المدنيين والعسكريين"

ومن الأهمية بمكان أن نشير هنا إلى مثال بسيط يوضح حجم الأضرار التي تخشى إسرائيل تكبدها جراء هجوم إلكتروني يستهدف مرافق البنى التحتية لديها، ألا وهي الأضرار الناجمة عن مهاجمة هيئة التحكم المحوسبة التي تشغل نظام الإشارات المرورية فيها.

فقد حذر أكثر من مسؤول إسرائيلي من أن أي طرف معادٍ قادرٍ على الولوج إلى وحدات التحكم الإلكتروني في نظام الإشارات المرورية يمكنه أن يتسبب في موت مئات الإسرائيليين خلال دقائق، حيث بإمكان هذا الطرف تغيير إعدادات هذه الوحدات، بحيث يتم تشغيل الأضواء الخضراء في نظام الإشارات المرورية

في الاتجاهات المتعاكسة في الوقت نفسه، مما يعني سقوط عدد كبير من القتلى والجرحى في حوادث طرق مؤكدة.

إن الأضرار الناجمة عن مهاجمة هيئة التحكم المحوسبة التي تشغل نظام الإشارات المرورية تعتبر بسيطة مقارنة بالأضرار الناجمة عن استهداف مرافق أكثر حيوية. فعلى سبيل المثال تخشى إسرائيل أن تتمكن أطراف "معادية" من الولوج إلى هيئات التحكم المحوسبة في مطار بن غوريون والتسبب في حوادث تصادم بين الطائرات المقلعة أو الهابطة، أو التشويش على النظم التي تتحكم في مستوى ارتفاع الطائرات أثناء اقتلاعها أو طيرانها حتى تصطدم ببعضها البعض، أو جعلها تصطدم بعوائق طبيعية.

وبواسطة الآلية ذاتها، يمكن المس بشكل جدي بتزويد الإسرائيليين بالكهرباء والماء وخدمات الاتصال المختلفة. وما ينطبق على المرافق المدنية يمكن أن ينطبق على المرافق العسكرية المختلفة التي توجه عبر هيئات تحكم محوسبة، وتحديداً مجمعات الصناعة العسكرية المختلفة.

فعلى سبيل المثال تخشى إسرائيل أن يتم التشويش على نظام رقابة وتحكم في مصنع ينتج وسائل قتالية بشكل يؤدي إلى تفجيره، علاوة على التأثير على هيئات التحكم المرتبطة بوسائل الدفاع الجوي لكي تستهدف طائرات عسكرية أو مدنية تعود لإسرائيل نفسها.

ويبلغ الفزع الصهيوني من النتائج "الكارثية" لحرب إلكترونية إلى حد الخوف من إمكانية أن تتمكن "الأطراف المعادية" من الوصول إلى النظم المحوسبة التي

تشغل مصانع البتروكيميائيات، والتي يمكن أن تؤدي إلى حدوث تفاعلات غير مرغوب فيها ينتج عنها سحب من الغازات السامة التي تؤدي إلى عدد كبير من القتلى، فضلاً عن الكوارث البيئية التي يمكن أن تنتج عن ذلك.

من هنا، فهي ترى أن المبادرات التي يقدم عليها الهاكرز لا تنجح في الغالب في الولوج إلى هيئات التحكم المحوسبة التي ترتبط بها مرافق البنى التحتية أو المنظومات العسكرية المختلفة لديها، على اعتبار أن الهاكرز غير مؤهل لاختراق منظومات الدفاع المرتبطة بهذه المنظومات.

إن الذي يجعل إسرائيل تبدي كل هذه الحساسية والمخاوف لخطر الحرب الإلكترونية يرجع بشكل أساسي إلى حقيقة إدراكها للطاقة الكامنة في الحرب الإلكترونية، على اعتبار أنها تمارس على نطاق واسع هذا النوع من الحرب في محاولتها تحقيق أهداف تكتيكية وإستراتيجية .

فلم يعد سراً أن إسرائيل تمكنت عام 2009 -بالتعاون مع الولايات المتحدة- من إعطاب أجهزة الطرد المركزي التي تعتمد عليها إيران في تخصيب اليورانيوم، وذلك عبر استخدام فيروس ."Stuxnet" ولم يتردد وزير الحرب الإسرائيلي الحالي موشيه يعالون في الاعتراف بأن إسرائيل هي المسؤولة عن الهجمة الإلكترونية التي تعرضت لها منظومات حواسيب إيرانية حساسة في يونيو/حزيران 2012، وذلك عبر استخدام فيروس."Flame"

"أنشأت إسرائيل هيئة الحرب الإلكترونية التابعة لرئاسة أركان الجيش, وتتمثل مهمتها في تنسيق وتخطيط العمليات الحربية في الفضاء الإلكتروني، وهي في ذلك تقتفي أثر الولايات المتحدة"

في الوقت ذاته، أقدمت إسرائيل على التسلل إلكترونياً إلى منظومات التحكم المسؤولة عن توجيه الدفاعات الجوية السورية عشية الغارة التي نفذتها الطائرات الإسرائيلية على المنشأة النووية السورية قرب دير الزور شمال شرق سوريا في سبتمبر/أيلول 2006، وأبطلت عمل هذه المنظومات حتى تقلصت فرص تعرض الطائرات المغيرة لنيران الدفاعات الجوية السورية.

وبالإضافة إلى هذا النوع العنيف من الاستخدام، فإن هناك توظيفا "ناعما" للحرب الإلكترونية تعكف عليه إسرائيل منذ سنين. فعناصر المخابرات الإسرائيلية يوظفون مواقع التواصل الاجتماعي في محاولاتهم لتجنيد عملاء عبر استخدام هويات مزيفة. وتؤكد المعطيات التي تقدمها الأجهزة الأمنية الفلسطينية أنه بالاستناد إلى التحقيقات التي أجريت مع أشخاص اعترفوا بالتعاون مع إسرائيل، يتبين أن نسبة كبيرة من هؤلاء أسقطوا في براثن العمالة لصالح إسرائيل بعد إقامة علاقات افتراضية مع رجال مخابرات قدموا أنفسهم على أنهم فلسطينيون عبر مواقع التواصل الاجتماعي.

من الواضح أن الحرب الإلكترونية أصبحت من الأدوات الرئيسية المستخدمة من قبل إسرائيل لتحقيق أهدافها الإستراتيجية دون التورط في مواجهة مكشوفة مع الأطراف المستهدفة، ومثال ذلك مهاجمة منظومات الحواسيب في المنشآت

النووية الإيرانية على اعتبار أنه ليس من السهولة تقديم أدلة قطعية تثبت مسؤولية طرف بعينه عن تنفيذ هجمات إلكترونية.

ولقد غدت الحرب الإلكترونية جزءاً لا يتجزأ من إستراتيجية إسرائيل الهجومية، حيث يتم توظيف الفضاء الإلكتروني في الجهد الحربي ضمن إستراتيجية شاملة اعتمدتها تل أبيب. فقد أقدم الجيش الإسرائيلي على خطوة مهمة جداً عندما أعلن عام 2009 أن الفضاء الإلكتروني بات يمثل إحدى المجالات الإستراتيجية العملياتية.

واستناداً إلى ذلك أقام الجيش "هيئة الحرب الإلكترونية" التي تتبع قيادة أركان الجيش الإسرائيلي، وتتمثل مهمة الهيئة في تنسيق وتخطيط العمليات الحربية في الفضاء الإلكتروني، وهي في ذلك تقتفي أثر الولايات المتحدة التي دشنت "هيئة الحرب الإلكترونية" التابعة لوزارة الدفاع الأميركية.

ففي 18 مايو/أيار 2011 أعلن رئيس الوزراء الإسرائيلي بنيامين نتنياهو عن تدشين "الهيئة القومية للحرب الإلكترونية"، وهدفها الأساسي اتخاذ الاستعدادات الدفاعية التي تمكن من حماية الفضاء الإلكتروني وحماية البنى التحتية والمرافق المدنية والعسكرية المرتبطة به. وحسب الإعلان، فإن الهدف من إقامة هذه الهيئة توسيع قدرات الدفاع في مواجهة أي حرب إلكترونية تشنها دول أو منظمات.

وتعتبر الهيئة مسؤولة عن جميع الأذرع العسكرية والمدنية المشاركة في هذا الجهد، وتعمل بتنسيق مع "السلطة الرسمية لحماية المعلومات" التابعة لجهاز

المخابرات الداخلية (شاباك)، وشركة "تهيلا" التي توفر خدمة تصفح للـوزارات والمؤسـسات التابعة لها.

إن القائمين على الهيئة يدركون أن التحدي الأبرز أمـامهم يتمثـل في تـصميم منظومـة دفـاع إلكترونية متكاملة، علما بأن بلورة مثل هذه المنظومـة يتطلـب تنـسيقا وتعاونـا كـاملا بـين المؤسسات المدنية والعـسكرية، بخـلاف مـا يتعلـق بالمجـال الحـربي التقليـدي الـذي تنفـرد بإدارته المؤسسة الأمنية.

وتنطلق الهيئة الجديدة من افـتراض مفـاده أن التنـسيق والتعـاون بـين المؤسـسات الأمنيـة والمدنية أمر بالغ الأهمية، لأنه من الصعب التمييز والتفريق في الفضاء الإلكتروني بين البنـى التحتية العسكرية والمدنية.

"ثمة دعوات في إسرائيل لإعادة صياغة العقيدة الأمنية التي بلورت مطلع خمسينيات القـرن الماضي، لكي تتلاءم مع الحرب في الفضاء الإلكتروني"

في الوقت ذاته ورغم أن المؤسسة الأمنية هي التي توجه الحـرب الإلكترونيـة ضـد الأطـراف الخارجية، فإنها تدرك أن تحـسين القـدرات الدفاعيـة يتطلـب تعاونـا وتنـسيقا مـع القطـاع الخاص، لاسيما شركات التقنية المتقدمة، على اعتبار أن لديها قدرات وكفاءات كبيرة في مجال التعامل مع الفضاء الإلكتروني.

لقـد وصـل الاهـتمام بـالحرب الإلكترونيـة في إسرائيـل إلى درجـة أن هنـاك دعـوات داخـل المؤسسة الأمنية ولجنة الخارجيـة والأمـن في الكنيـست إلى إعـادة صـياغة العقيـدة الأمنيـة الإسرائيلية التي بلورت مطلع خمسينيات القرن المـاضي لـكي تـتلاءم مـع الحـرب في الفـضاء الإلكتروني.

وأخيرا, فإن تفوق طرف ما في مجال الحرب الإلكترونيـة يتوقـف بـشكل أسـاسي عـلى مـدى قدرته على توظيف واستغلال موارده الذاتيـة، وخاصـة البـشرية. فـإن كـان طـرف عـربي أو إسلامي معني برد الصاع صاعين لإسرائيل في مجال الحرب الإلكترونية، فإن عليه الاستثمار في مجال إعداد الكادر البشري الملائم، مع كل ما يتطلبه ذلك من وجود بيئـة تعليميـة تـضمن المخرجات المطلوبة.

ومن نافلة القول إن النظم السياسية الوطنية الديمقراطية هي تلك التـي تحـرص عـلى بـذل أقصى جهد ممكن في توظيف موارد بلدانها الذاتية.

حرب الفضاء الالكتروني وإسرائيل

وقد تعاظم في الفترة الأخيرة اهتمام مراكـز الأبحـاث والنخـب في إسرائيـل بموضـوع الحـرب في الفـضاء الالكـتروني. ونظـم معهـد أبحـاث الأمـن القـومي التـابع لجامعـة تـل أبيـب، في التاسـع مـن حزيـران/ يونيـو 2011، يومـاً دراسـياً تنـاول هـذا الموضـوع، وتحـت عنـوان "حـرب الفـضاء الالكـتروني - تحـديات عـلى الـصعيد العـالمي والـسياسي والتكنولـوجي". وافتتح اليوم الدراسي رئيس الحكومة الإسرائيلية بنيـامين نتنيـاهو، وتحـدث فيـه نخبـة مـن البـاحثين والمختـصين الإسرائيليـين، الـذين أكـدوا عـلى أهميـة الحـرب في الفـضاء الالكـتروني بالنـسبة لأمـن إسرائيـل. وشـدد بنيـامين نتنيـاهو في مداخلتـه عـلى أهميـة وحيويـة هـذا الموضوع بالنـسبة لإسرائيـل، وأكـد عـلى ضرورة أن تـصبح إسرائيـل دولـة عظمـى في مجـال حـرب الفـضاء الالكـتروني، وأن تكـون فـاعلاً هامـاً عـلى الـصعيد العـالمي في هـذا المـضمار كما ناقشت "لجنـة العلـم" التابعـة للكنيـست في الرابـع مـن تمـوز/ يوليـو 2011 موضـوع

الحرب في الفضاء الالكتروني، واستمعت إلى الخبراء والمختصين في هذا المجال.

وأشار الجنرال البروفيسور يتسحاق بن يسرائيل، رئيس "المجلس الوطني للبحث والتطوير" أمام "لجنة العلم"، إلى وجود فجوة في إسرائيل بين الاحتياطات الدفاعية عن البنى التحتية الأمنية وبين الدفاع عن بنى تحتية مدنية حساسة وهامة ضد هجمات في الفضاء الالكتروني. وأضاف أن الهجمات في الفضاء الالكتروني تحدث يومياً وأنها ليست جزءا من الخيال العلمي بل هي حقيقة واقعة. واستطرد قائلا: "جزء من هذه الهجمات يسبب ازعاجاً، بينما قد يلحق الجزء الآخر من هذه الهجمات أضراراً جسيمة. فهناك الكثير من البرامج والأنظمة المتطورة التي يمكن استعمالها في الفضاء الالكتروني التي قد تشل وتعطل عمل مرافق الدولة الأساسية مثل: البورصة والبنوك والكهرباء والمواصلات والاتصالات، والناس لا يدركون عمق الخطر".

وأشار يتسحاق بن يسرائيل إلى أن أحد أهداف إقامة "هيئة السايبر الوطنية" في إسرائيل، التي أعلن عن تأسيسها في أيار/ مايو 2011، هو إنشاء "الحاسوب المتطور" في إحدى الجامعات بإسرائيل، إذ لا تملك إسرائيل مثل هذا الحاسوب، ويحظر بيعه إليها، لعدم توقيعها على اتفاقية حظر انتشار الأسلحة النووية. أما رئيس "لجنة العلم" التابعة للكنيست، مئير شطريت، فقال في سياق تشديده على موضوع تأمين الفضاء الالكتروني، إنه بالإمكان التسبب في انهيار إسرائيل من دون دبابات وطائرات، وإنما بواسطة حرب الفضاء الالكتروني

وفي سياق هذا الاهتمام الإسرائيلي بحرب الفضاء الالكتروني صدر باللغة العبرية، في حزيران/ يونيو 2011، عن معهد أبحاث الأمن القومي التابع لجامعة تل أبيب، كتاب "حـرب الفـضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل"، للبـاحثين شـموئيل ايفـن ودافيـد بـن سـيمان- طوف، العاملين في معهد أبحاث الأمن القومي. ويضم الكتاب مقدمة وأربعة فصول وخاتمة وملحقين، بما مجموعه تسعين من الصفحات. وأشار المؤلفان إلى أن الفـضاء الالكـتروني بـات مجال قتـال جديـد، وانـضم بـذلك إلى مجـالات القتـال الأخـرى، في اليابـسة والبحـر والجـو والفضاء. فالدول المتطورة وجيوشها تزيد من نشاطاتها وأبحاثها في الفضاء الالكـتروني الـذي أصبح يشكل بالنسبة لها مـصدر قـوة عظيمـة، ولكنـه في الوقـت نفـسه يكـشف خاصرتهـا الضعيفة، لأن البنى التحتية التي تقوم عليها الدول الحديثة مثل الكهرباء والمياه والمواصلات والاتصالات والبورصـة والبنـوك تعتمـد في عملهـا عـلى الفـضاء الالكـتروني. وكـذلك شـبكات القيادة والـسيطرة والـتحكم العـسكرية ومختلـف أنـواع التكنولوجيـا المتطـورة في سـاحات القتال؛ مثل: أنظمة جمع المعلومات، واستعمال الأقمار الصناعية والطائرات مـن دون طيـار في الحرب؛ كلها تعتمد على الفضاء الالكتروني.

ونوه المؤلفان إلى ميزات الفضاء الالكتروني كمجال قتال، وأبرزها التمكن من العمـل بـسرعة واحد من الألف من الثانية، ضد أعداء يبعدون آلاف الأميال مـن دون تعـرض المهـاجمين أو المقاتلين للأخطار.

والميــزات التــي يتمتــع بهــا الفــضاء الالكــتروني تجعلــه جــذاباً للاســتعمال في القتــال خــلال الحــرب، إلى جانــب الأســلحة التقليديــة، مــثلما فعلــت روســيا، كــما يقــول

المؤلفان، في حربها ضد جورجيا في سنة 2008. ويمكن أيضا استخدامه أثناء الحرب ضد أهداف استراتيجية، مثل الهجوم الذي تعرض له المفاعل النووي الإيراني في سنة 2009، حيث اعتبر المؤلفان أن هذا الهجوم (الذي قامت به إسرائيل وفق العديد من المصادر الإعلامية) كان حدثا تأسيسياً في مجال حرب الفضاء الالكتروني، وشكل مرحلة جديدة في تطور استعمال الفضاء الالكتروني في مجال القتال.

واعتبر المؤلفان أن استعمال الفضاء الالكتروني في القتال وعمليات التطوير والاستعدادات التي قامت بها دول عديدة، يؤكد أن سباق التسلح في مجال الفضاء الالكتروني قد بدأ. ويشيران إلى أن العديد من الدول أقامت في السنوات الأخيرة مؤسسات وهيئات مختلفة ومختصة باستعمال الفضاء الالكتروني كمجال قتال، وطورت استراتيجيات أمنية في الفضاء الالكتروني.

وبدأ المؤلفان الفصل الأول الذي جاء تحت عنوان "الفضاء الالكتروني والمجال الأمني - إطار مصطلحي"، بتعريف وشرح المصطلحات المتعلقة بموضوع الفضاء الالكتروني. ثم عالجا في هذا الفصل المواضيع التالية: ميزات الفضاء الالكتروني كمجال للحرب، الفضاء الالكتروني - مصطلحات أمنية تقليدية مع مضمون جديد، البيئة الاستراتيجية للفضاء الالكتروني، التجسس والحرب الالكترونية الرخوة، وحرب الفضاء الالكتروني.

وحمل الفصل الثاني عنوان "عمليات هجومية وعوامل كابحة في الفضاء الالكتروني"، وشمل المواضيع التالية: عمليات هجومية بارزة في الفضاء الالكتروني، العوامل التي قادت إلى زيادة المعرفة في الفضاء الالكتروني،

استعمال الفضاء الالكتروني لأغراض الحرب - العوامل الكابحة، الإرهاب في الفضاء الالكتروني، ميثاق دولي لتنظيم النشاط في الفضاء الالكتروني، وتلخيص للعوامل المشجعة والعوامل الكابحة لاستعمال سلاح حرب الفضاء الالكتروني في الصراعات بين الدول.

وعالج الفصل الثالث الذي جاء تحت عنوان "نظرة إلى ما وراء البحر - استعداد دول لتحدي الفضاء الالكتروني"، استعدادات العديد من الدول الهامة واستراتيجياتها والمؤسسات التي أقامتها من أجل ضمان أمنها أمام المخاطر الكامنة في الفضاء الالكتروني، وهذه الدول هي: الولايات المتحدة وفرنسا وألمانيا وبريطانيا والصين.

عالج الباحثان في الفصل الرابع أهمية وحيوية الفضاء الالكتروني لإسرائيل والتدابير المؤسساتية التي اتخذتها إسرائيل لحماية فضائها الالكتروني. وقدما اقتراحا حول الاستراتيجية التي ينبغي على إسرائيل اتباعها للدفاع عن فضائها الالكتروني. كما عالجا كيفية دمج الفضاء الالكتروني باستراتيجية الأمن الإسرائيلي.

وأشار المؤلفان إلى أن إسرائيل باتت دولة "محوسبة" تعتمد مؤسساتها الحكومية ومختلف المرافق والشركات فيها على شبكة الإنترنت. كما تتم الكثير من معاملات المواطنين فيها مع مؤسسات الدولة والمرافق المختلفة في الدولة بوساطة شبكة الإنترنت. وأكد الباحثان أن تكنولوجيا المعلومات تساهم مساهمة مباشرة وغير مباشرة في نمو الاقتصاد الإسرائيلي، إذ تعتبر إسرائيل من ضمن مجموعة الدول العديدة المتقدمة في تطوير تكنولوجيا المعلومات. وقد بلغ حجم

اقتصاد الإنترنت في إسرائيل في سنة 2009 خمسين مليار شيكل (الدولار يساوي ثلاثة شيكل ونصف)، وهو ما يعادل 6.5 في المئة من مجمل الانتاج المحلي الإسرائيلي. ومن المتوقع أن يبلغ اقتصاد الإنترنت في إسرائيل في سنة 2015 خمسة وثمانين مليار شيكل، وهو ما سيعادل 8.5 في المئة من مجمل الإنتاج المحلي الإسرائيلي.

تدابير إسرائيل للدفاع عن فضائها الإلكتروني

ذكر المؤلفان أن إسرائيل اتخذت مجموعة من التدابير خلال العقد ونصف العقد الأخيرين من أجل حماية الفضاء الالكتروني والدفاع عنه، وأهم هذه التدابير:

أولاً: البنية التحتية الحكومية لعصر الإنترنت

أقامت إسرائيل في سنة 1997 مشروع "بنية الحكومة التحتية لعصر الإنترنت" في داخل وزارة المالية الإسرائيلية. وحدد هدف هذا المشروع في حماية وتأمين استعمال الإنترنت في الوزارات والمؤسسات الحكومية. وأقيم داخل هذا المشروع "مركز حماية المعلومات لحكومة إسرائيل" وأنيطت به مهام متابعة تطور وسائل حماية المعلومات في العالم والتنسيق بين الوزارات والمؤسسات الحكومية من أجل إيجاد حلول لمشاكل حماية المعلومات وكذلك إجراء أبحاث حول هذا الموضوع.

ثانياً: السلطة الرسمية لحماية المعلومات

أنشئت في سنة 2002 "السلطة الرسمية لحماية المعلومات"، في داخل جهاز المخابرات العامة (الشاباك). وأنيط بهذه السلطة مهام حماية البنى التحتية

للحواسيب الهامة والحيوية في إسرائيل من مخاطر ما أطلق عليه "تهديدات إرهابية" و"عمليات تخريب" ونشاطات تجسسية. وأشار المؤلفان إلى وجود لجنة تابعة لمجلس الأمن القومي الإسرائيلي، والتي تقع من بين صلاحياتها السماح لـ"السلطة الرسمية لحماية المعلومات" التابعة لجهاز المخابرات العامة (الشاباك) بتوسيع قائمة المؤسسات التي تقوم بمراقبتها بغرض حماية المعلومات فيها. وذكر المؤلفان أن عمل "السلطة الرسمية لحماية المعلومات" تعتريه العديد من النواقص، لكونه لا يشمل جميع المؤسسات والمنشآت في إسرائيل ولأن هذه السلطة تابعة لجهاز المخابرات العامة (الشاباك)، ما يردع الكثير من المؤسسات من التعامل والتفاعل معها بحرية وأريحية.

ثالثاً: هيئة السايبر في الجيش الإسرائيلي

في سنة 1909، اعتبر غابي اشكنازي رئيس هيئة أركان الجيش الإسرائيلي الفضاء الالكتروني كمجال قتال من الناحيتين الاستراتيجية والعملياتية. وبناء على ذلك أقام الجيش الإسرائيلي "هيئة السايبر" في الوحدة 8200 في جهاز المخابرات العسكرية الإسرائيلية (أمان)، بغرض توجيه وتنسيق نشاطات الجيش الإسرائيلي في الفضاء الالكتروني. وفي كانون الأول/ ديسمبر 2009، أشار عاموس يادلين، رئيس جهاز المخابرات العسكرية الإسرائيلية حينئذ، في محاضرة له في معهد أبحاث الأمن القومي، إلى أن أحد أهم الأخطار التي تتربص بإسرائيل وقد تلحق بها الأذى، تكمن في احتمال اختراق الحواسيب الحيوية الإسرائيلية. وأوضح عاموس يادلين، أن هيئة السايبر في الجيش

الإسرائيلي تهدف إلى توفير دفاع جيد لشبكات الأنترنت العاملة في إسرائيل، وكذلك القيام بهجمات في الفضاء الالكتروني على أهداف خارجية.

رابعاً: وحدة إدارة أنظمة المعلومات

صادقت الحكومة الإسرائيلية في 27 أذار/ مارس على إقامة "وحدة إدارة المعلومات"، وهي تتبع مدير عام وزارة المالية الإسرائيلية ومسؤولة مسؤولية مباشرة على جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك عن مشروع "بنية الحكومة التحتية لعصر الإنترنت".

خامسا: هيئة السايبر الوطنية

أعلن رئيس الحكومة الإسرائيلية بنيامين نتنياهو في 18 أيار/ مايو 2011 عن إنشاء "هيئة السايبر الوطنية" في إسرائيل. وذكر نتنياهو أن الهدف الأساس لهذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن أنظمة البنى التحتية الحيوية، من "هجمات إرهابية" في الفضاء الالكتروني، التي قد تقوم بها دول أجنبية أو "منظمات إرهابية". ووفق ما ذكره نتنياهو، فإن إسرائيل مكشوفة لهجمات في الفضاء الالكتروني، فكل ما هو محوسب فإنه قد يتعرض للهجمات في الفضاء الالكتروني، التي قد تشل أنظمة مرافق ومؤسسات حيوية للغاية التي تشغل الدولة مثل: الكهرباء والمياه والاتصالات والمواصلات.

ويشير المؤلفان إلى أنه علاوة على مهامها الدفاعية عن الفضاء الالكتروني الإسرائيلي ، فإن من مهام "هيئة السايبر الوطنية" تشجيع وتطوير شركات إسرائيلية مختصة في الدفاع عن الفضاء الالكتروني، بغرض الحصول على

جزء من سوق الفضاء الالكتروني الذي ينمو بسرعة كبيرة للغاية على الصعيد العالمي.

وأوضح الكاتبان أن ثلاثة عوامل هامة تدفع إسرائيل للإسراع في اتخاذ الاحتياطات والتدابير الأمنية في الفضاء الالكتروني، وهي:

أولاً: كدولة متطورة ومرافقها ومؤسساتها محوسبة، يتعرض الفضاء الالكتروني في إسرائيل إلى أخطار حدوث هجمات عليه، قد تؤدي إلى إلحاق الشلل بالبنى التحتية الإسرائيلية.

ثانياً: تواجه إسرائيل أعداء لهم دوافع لإلحاق الأذى بها كلما استطاعوا تحقيق ذلك، سواء من قبل دول أو منظمات أو أفراد.

ثالثا: هناك فرصة أمام إسرائيل ليس فقط لتطوير دفاع متقدم في الفضاء الالكتروني وإنما أيضا لاستعمال الفضاء الالكتروني في الحرب.

استراتيجية للدفاع عن الفضاء الالكتروني الإسرائيلي

اقترح المؤلفان أن تتبنى الحكومة الإسرائيلية استراتيجية وطنية للدفاع عن الفضاء الالكتروني الإسرائيلي وفق الخطوط التالية:

1. الاعتراف بالفضاء الالكتروني كمجال وطني جديد، الذي ينبغي الدفاع عنه بشكل خاص (إلى جانب المجالات الأخرى: البر والبحر والجو)، من خلال رؤية شاملة وتعاون جميع الأطراف ذات الصلة.

2. تأسيس مؤسسة وقيادة مركزية للدفاع عن الفضاء الالكتروني على المستوى الوطني.

3. وضع البنى التحتية الحيوية وأنظمة الأمن في قمة الأولويات، وفي الوقت نفسه القيام بالدفاع عن مركبات أخرى، مثل الدفاع عن المعلومات في الجامعات ومراكز الأبحاث والدفاع عن شركات لها تأثيرها على الاقتصاد الإسرائيلي ولكنها ليست مصنفة كجزء من البنى التحتية.

4. بناء نظام دفاعي دينامي وشامل في الفضاء الالكتروني مثل النظام الذي أقامته وزارة الدفاع الأميركية.

5. التعاون الدائم في مجال الفضاء الالكتروني بين القطاع الحكومي والقطاع الأمني والقطاع الخاص.

6. التعاون مع دول أجنبية بشأن الفضاء الالكتروني، وخاصة الدول الحليفة.

7. سن قوانين خاصة بالفضاء الالكتروني والقيام بتطبيقها على أرض الواقع.

8. مساعدة الجمهور العام في زيادة الوعي بالفضاء الالكتروني وتطوير قدراته في الدفاع في هذا المجال، ومنح محفزات للشركات والأفراد لشراء برامج دفاع، وزيادة الرقابة على شركات الحماية.

9. استعمال الوسائل والأجهزة التكنولوجية الأكثر تطورا المتعلقة بالفضاء الالكتروني.

10. بلورة وتطوير سياسة ردع إسرائيلية، بما في ذلك قدرة الرد المباشر ضد كل من يهاجم الفضاء الالكتروني الإسرائيلي وإلحاق الأذى به، وهذا الأمر من مهام المؤسسة الأمنية الإسرائيلية.

الفضاء الالكتروني في استراتيجية الأمن الإسرائيلي

يؤكد المؤلفان أن إضافة الفضاء الالكتروني كساحة قتال جديد، إلى جانب ساحات القتال في البر والبحر والجو والفضاء، يستوجب دمج الحرب في الفضاء الالكتروني في استراتيجية ومفهوم الأمن الإسرائيلي؛ وهو ما يستوجب استحداث تغييرات في مفاهيم المصطلحات الأساسية المتعلقة بنظرية الأمن الإسرائيلي. فمثلا تختلف "البيئة الاستراتيجية" في الفضاء الالكتروني عن المفهوم التقليدي لها في نظرية الأمن الإسرائيلي القائم على التهديدات الجيو-سياسية التقليدية. علاوة على ذلك، يختلف الزمان والمسافة والمساحة في الفضاء الالكتروني عن المفاهيم التقليدية، لأن سرعة العملية الهجومية في الفضاء الالكتروني، ضد هدف يبعد مئات أو آلاف الأميال، تبلغ واحد على الألف من الثانية. ويرى المؤلفان أنه من الصعب للغاية أن تقوم إسرائيل بتطبيق سياسة الردع، التي تعتبر حجر الزاوية في سياسة الردع الإسرائيلية، في حرب الفضاء الالكتروني، لصعوبة تحديد هوية الطرف المهاجم في حرب الفضاء الالكتروني.

ويقول صاحبا الكتاب أن الدفاع في حرب الفضاء الالكتروني يـشكل تحـدياً مـن نـوع جديـد لإسرائيل، وذلك لأنه بمقدور العدو شن هجمات بسرعة البرق ومن الـصعوبة بمكـان تحديـد من هو المهاجم. ويوصي المؤلفان أن تتعلم إسرائيل وتستفيد من مفهوم "الدفاع الفعـال" في الفضاء الالكتروني الذي تتبعه الولايات المتحدة الأميركية. إذ يستند هذا "الدفاع الفعال" على قدرة مخابراتية متطورة لتحديد النشاطات في لإنترنت وعلى أنظمـة دفـاع ديناميـة ذات رد تلقائي من دون تدخل الإنسان. ويستطرد المؤلفان، إن "الدفاع الفعال" لا يعتمد فقـط عـلى التكنولوجيا المتطورة، وإنما أيضا على شـبكة محكمـة ذات قواعـد وإجـراءات صـارمة وعـلى ثقافة تفهم المخاطر وعلى انضباط شديد وعلى حماية المواقع وعلى رقابة بشرية قوية.

و في ضوء اعتراف الجيش الإسرائيلي بالفضاء الالكتروني كـساحة قتـال يـوصى المهتمـون مـن الجانب الإسرائيلي إلى جانب الساحات الأخرى، بإجراء تغييرات في قوات الجـيش الإسرائـيلي والعمل على إقامة جيش خاص بالفضاء الالكتروني، أسوة بالقوات البرية والبحرية والجوية.

الفصل الخامس

منظومة الحرب الإلكترونية في غزو العراق

مقدمة عامة

منظومات الحرب الالكترونية التي جرى استيرادها او تصنيعها وتطويرها داخل العراق، والتي تعتبر من اهم حلقات التكنولوجيا وأكثرها تقدما وتعقيدا والتي من خلالها تمكن العراق من مُجاراة اخر ما توصلت اليه دول العالم المتقدمة في التكنولوجية الالكترونية. حيث سنتكلم عن منظومات التشويش الالكتروني ضد طائرات وصواريخ العدو التي جرى تصنيعها اعتمادا على الامكانات والقدرات العراقية وتلك التي شارك خبراء اجانب في تصنيعها وتطويرها داخل العراق. كمنظومات التضليل على الصواريخ المضادة للرادار والصواريخ والقذائف الموجهة بالأقمار الصناعية او بالأشعة تحت الحمراء، او المنزلقة على الليزر، فضلا عن منظومة التحكم والسيطرة على طائرات البريداتور فائقة التطور المسيرة عن بعد، ناهيك عن منظومات التشويش على طائرات الاواكس (AEWC) وأقمار التجسس "نافستار" التابعة لوزارة الدفاع الأمريكية. كما سنشير الى نظام الرادار المحمول جوا من طراز بغداد وعدنان اللذان جرى تصنيعهما في الثمانينات واللذان يعتبران من اهم وسائل الحرب الالكترونية وأكثرها تعقيدا وتطورا، وذلك من باب الالمام الكامل ببرامج الدفاع الجوي العراقي.

وهنا نود ان نجدد ما سبق وذكرناه في الحلقة الرابعة، حيث حرصنا على ذكر بعض التفاصيل التي لم يتم التطرق لها سابقا حتى من قبل الاخ محب المجاهدين نفسه، حيث سيجد القارئ الكريم نفسه ولأول مرة امام بحث متكامل الاوجه دقيق التفاصيل مدعم بالصور والمعلومات والوثائق والمستندات

الاخبارية، كما سبق ونشرنا ملحق خاص للتعريف بأهم المصطلحات العلمية والعسكرية التي يتكرر ذكرها في بحثنا هذا. وكل ذلك من اجل ان تتمكنوا من الالمام الكامل والتام بما نتحدث عنه هنا، فرجائنا منكم قرائنا الافاضل ان تتوخوا الدقة والتركيز والانتباه في قراءتكم لهذه الحلقة.

منظومات الحرب الالكترونية :

يعد هذا الميدان من احدث وسائل الحرب وأكثرها تقدما وتعقيدا، وهي مجموعة الإجراءات الإلكترونية المتضمنة اولا استخدام بعض النظم والوسائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم العدو ووسائله ومعداته الإلكترونية المختلفة (أي عمليات المراقبة الالكترونية) مع الاستخدام المتعمد للطاقة الكهرومغناطيسية في التأثير على هذه النظم والوسائل لمنع العدو أو حرمانه أو تقليل استغلاله للمجال الكهرومغناطيسي (أي عمليات التشويش او الاعاقة الالكترونية) فضلاً عن حماية الموجات الكهرومغناطيسية الصادرة من النظم والوسائل الإلكترونية الصديقة من استطلاع العدو لها أو التأثير عليها(أي عمليات الحماية الالكترونية).

لم يكن هذا النوع من الحرب المتطورة غائبا عن ذهن الخبراء العراقيين المختصين بالدفاع الجوي العراقي مثلما لم تغفل القيادة العراقية اهمية هذا السلاح الحيوي، ونظرا للدمار الهائل الذي لحق بالقوة الجوية والدفاع الجوي العراقيين وتضائل قدراتهما عقب حرب عام 1991، وبعد عدة محاولات فاشلة قامت بها الطائرات ومنظومات الدفاع الجوي العراقية في التصدي للطائرات الامريكية والبريطانية والفرنسية التي اخذت على عاتقها مهمة فرض منطقتي

حظر الطيران، ومن اجل ايقاف الاستنزاف الكبير الذي يتعرضـان لـه، فقـد وجهـت القيـادة العراقية قوتها ودفاعاتها الجوية ومنذ عام 1993 بتجنب الاشتباك المباشر مع طائرات العدو والاعتماد على وسائل اخرى تضمن المحافظة على العنـصر البـشري والمـادي للـدفاع الجـوي العراقي، وهو ما اضطلع به خبراء الحرب الالكترونية الذين اثبتـوا كفـاءتهم في هـذا المجـال التكنولوجي بالغ التعقيد منذ الثمانينيات حيـث نجحـوا في تـصنيع اربعـة منظومـات رادار للسيطرة والإنذار المبكر المحمولة جواً - الاواكس من طراز بغداد وعدنان.

امـا في التـسعينيات ورغـم الحـصار الـشامل الـذي فـرض عـلى العـراق، فقـد اصر الخـبراء العـراقيين في الحـرب الالكترونيـة عـلى مواصـلة جهـودهم ومثـابرتهم لمواكبـة التطـور السريع الحاصـل في هـذا الميـدان الحـربي والتكنولـوجي بـالغ التطـور والتعقيـد. فمـما قـد لا يعرفه الكثيرين وعلى الرغم من التفوق الالكتروني الكبير الذي تمتـع بـه العـدو الامـريكي، والتفـوق التقنـي الهائـل الـذي تمتعـت بـه طائراتـه القاصـفة والإسـتراتيجية وطـائرات الانذار المبكر والاستطلاع الميـداني والعميـق، وصـواريخه الجوالـة وقذائفـه الذكيـة المنزلقـة عـلى الليـزر والموجهـة بـالأقمار الـصناعية، نقـول عـلى الـرغم مـن كـل ذلـك فقـد كـسب الـدفاع الجـوي العراقـي العديـد مـن الجـولات واسـتطاع الخـبراء العراقيـون في الحـرب الالكترونية وبنجاح باهر مـن التـصدي لمجموعـة كبـيرة مـن أسـلحة العـدو فائقـة التقـدم، قبل الغزو وبعده. حيث تمكنوا مـن اسـقاط وتـدمير المئـات مـن طـائرات العـدو الامـريكي مـــما اجـــبره عـــلى اخـــراج مـــا تبقـــى منهـــا مـــن الخدمـــة العـــسكرية في صـــفوف

قواته الغازية للعراق العظيم، ناهيك عن نجاحهم الباهر في تشتيت صواريخ العدو الذكية بل وتوجيهها نحو قوات العدو هو نفسه.

1- منظومة السيطرة والإنذار المبكر المحمولة جواً / الاواكس العراقية :

في ثمانينيات القرن العشرين ومع اندلاع الحرب العراقية الايرانية وعلى اثر الغارة الجوية التي شنتها طائرات العدو الصهيوني على مفاعل تموز النووي، فقد برزت حاجة العراق لامتلاك رادار متطور قادر على رصد الاهداف الجوية المعادية التي لا تستطيع رادارات الدفاع الجوي العراقي التقليدية من اكتشافها كما هو الحال بالنسبة للطائرات المعادية التي تحلق على ارتفاع منخفض.

أ - منظومة السيطرة والإنذار المبكر بغداد – 1 المحمولة جوا:

بسبب عزوف الدول المصنعة لهكذا انواع من الرادارات والتي تعتبر من الوسائل العسكرية الاكثر تطورا وأهمية، وعلى اثر تراكم الخبرات العلمية لدى خبراء وفنيي العراق عموما والعاملين في هيئة البحث العلمي والتطوير الفني في القوات المسلحة خصوصا، ومع النجاحات الكبيرة التي شهدتها هذه المؤسسة الكفوءة منذ تأسيسها عام 1983 حتى اصبحت في عام 1985 مؤسسة علمية صناعية متكاملة عرفت بهيئة التصنيع العسكري والتي كان لعطاء منتسبيها اثره الكبير في عراقنا المجاهد حتى يومنا هذا، فقد وجهت القيادة العراقية خبرائها في الدفاع الجوي والحرب الالكترونية نحو تصنيع رادار محمول جوا يعمل كمنظومة سيطرة وإنذار مبكر لدعم كافة صنوف القوات المسلحة العراقية وبالأخص قوات الدفاع الجوي العراقي.

وبالفعل فقد نجحت مجموعة خيرة من الخبراء والفنيين العراقيين كان من بينهم العالم العراقي الكبير الفريق عامر محمد رشيد العبيدي، وبفترة قياسية لم تتجاوز الستة اشهر خلال عام 1987 من تحوير رادار (TIGER) فرنسي المنشأ كان يستخدم كرادار ارضي يعمل وفق مبدأ دوبلر لكشف الطائرات المعادية المحلقة على ارتفاعات واطئة وحتى ارتفاع 6.000 متر من على بعد 120 كم، ليصبح اول رادار عراقي محمول جوا سمي بغداد -1. وقد اعتمد الخبراء العراقيين على تركيب اربعة هوائيات داخل قبة مصنوعة من مادة الفايبر كلاس في الجزء الخلفي من طائرة شحن جوي عائدة لشركة الخطوط الجوية العراقية طراز انتونوف 76 (IL-76MD) روسية المنشأ بدلا من باب الشحن، وبواقع هوائيين اثنين في كل جانب وقد استطاعت هذه المنظومة من تامين مسح راداري بزاوية 180 درجة ولمدى 350 كم.

طائرة الشحن الجوي طراز انتونوف 76 (IL-76MD) التي ركب الخبراء العراقيون منظومة رادار بغداد 1 و 2 في الجزء الخلفي منها.

ب - منظومة السيطرة والإنذار المبكر بغداد – 2 المحمولة جوا :

على اثر نجاح الخبراء العراقيين في انجاز منظومة رادار بغداد – 1 ومن اجل زيادة المسح الراداري لها، فقد واصل الخبراء العراقيين جهودهم لتطوير المنظومة العراقية المحمولة جوا بحيث تكون قادرة على تامين مسح راداري كامل بزاوية 360 درجة، وبالفعل وخلال ستة اشهر اخرى انجز الخبراء

العراقيين تركيب هوائيين اضافيين اثنين في الطائرة ليصبح عدد الهوائيات التي تم تركيبها في الطائرة ستة هوائيات، تم تركيب الهوائي الخامس في مقدمة الطائرة، بينما تم تركب الهـوائي السادس في نهاية جسم الطائرة، وبهذا الانجاز العلمي الجديد فقد استطاع الـرادار العراقـي الثاني المحمول جوا الذي سمیى بغداد – 2 من تامين مسح راداري كامل بزاويـة 360 درجـة ولمدى 350 كم ايضا. وقد تم نقل طائرة بغداد – 2 الى ايران قبيل حرب عـام 1991 وأصرت الحكومة الايرانية على عدم ارجاعها للعراق حتى يومنا هذا.

طائرة الشحن الجوي طراز انتونوف 76 (IL-76MD) التي ركب الخبراء العراقيون هوائيات منظومة رادار بغداد 2 داخل قبة مصنوعة من الفايبر كلاس في الجزء الخلفـي مـن الطـائرة والتي تصر الحكومة الايرانية منذ 23 عاما على عدم ارجاعها الى العـراق ويتـضح في الـصورة اللون القديم للطائرة العراقية التي كانت جزءا من الخطوط الجوية العراقية .

ج - منظومة السيطرة والإنذار المبكر عدنان – 1 المحمولة جوا :

على اثر نجاح اسرائيل في تصنيع رادار محمـول جـوا يعمـل كمنظومـة سـيطرة وإنـذار مبكـر والتي اعتمد الخبراء الاسرائيليين على الهوائيات ايضا بدل الصحن المدور، حيث تم تركيب ستة هوائيات وزعت على جسم الطائرة اثنان على كل جانب وواحـد في المقدمـة وآخـر في مـؤخرة الطائرة وتؤمن مسح راداري بزاوية 360 درجة وقد أستغرق العمـل بهـذا النمـوذج أكـثر مـن ثلاث سنوات وبلغت كلفته نحو 70 مليون دولار. فقد وجهت القيـادة العراقيـة التـي تهـدف دائما للتفـوق عـلى قـدرات العـدو الـصهيوني نحـو تـصنيع منظومـة رادار محمولـة جـوا اكـثر

تطورا شبيها بطائرة الاواكس (Sentry.E3) التي تتفاخر الولايات المتحدة الامريكية بها منذ نهاية السبعينيات كونها تعتبر من احدث التقنيات الالكترونية وأكثرها تطورا وتعقيدا.

زودت طائرة الاواكس برادار متقدم مرتبط بأربع هوائيات وضعت في وعاء قطـره 7.32 م داخل صحن دوار يبلغ قطره 9.1 متر وسمكه نحـو 1.8 مـتر ويـزن نحـو 2.000 كغـم ركـب فوق جسم طائرة بوينغ 707 يدور بمعدل 6 دورات في الدقيقة الواحـدة، وذو مستـشعرات كهرومغناطيسية فائقة التطور جعلت الاواكس قـادرة عـلى رصـد مختلـف انـواع الاهـداف الجوية وحتى البرية كالعجلات التي تسير في شوارع المدن ومن على مسافة 480 كم وبزاوية 360 درجة، وعرض صورها الملونة على شاشات الرادار الـ 14 التي تم تركيبهـا مـع مجموعـة كمبيوترات فائقة التقنية ركبت داخل جسم الطائرة وتجـري 740 ألـف عمليـة حـسابية في الثانية الواحدة، كما زودت بأجهزة اتصال ومراقبة متطورة جدا تـستطيــع اكتـشاف وتتبّـع 250 هـدف في آن واحـد، وزودت الاواكـس بجهـاز (IFF) لتمييـز الطـائرات الـصديقة مـن المعادية. كما تحتـوي الاواكـس عـلى 18 جهـاز اتـصال متطـور ، 3 اجهـزة اتـصال تـستخدم الموجات اللاسلكية عالية التردد (HF)، و 12 جهاز اتصال يستخدم الموجات اللاسـلكية جـدا عاليـة الـتردد (VHF)، وجهـازين يـستخدمان الموجـات اللاسـلكية فـوق عاليـــــة الـتردد (UHF) إضافة إلى وصلة معلومات رقميـــة ذات سرعـة عاليــة، كـما تـم تركيـب منظومـة مضادة للتشويش من اجل تأمين استمرار سريان المعلومـات وسِريتهـا، كـما زودت طـائرات الاواكس بتقنية التزود بالوقود جوا.

لذا فان طائرة الاواكس تعد واحدة من اكثر وسائل الحرب الحديثة استخداما، حيث تقوم بمختلف مهام الحرب الالكترونية من استطلاع ورصد ومراقبة وتشويش فضلا عن قدرتها لتامين الحماية الالكترونية لباقي الطائرات والرادارات الارضية وحتى القطع البحرية. كما تتيح طائرة الاواكس المجال امام قادة الجيش للتحكم بمسرح العمليات الحربية عن بعد والتنسيق بين مختلف صنوف الجيش.

وفقا لتوجيهات القيادة العراقية، فقد باشر الخبراء العراقيين الدخول في واحد من اكثر المشاريع العلمية تطورا وتعقيدا حيث وجد الفريق الفني العراقي نفسه امام كم هائل من الاسرار التكنولوجية فائقة التعقيد لاسيما وان وزن الصحن الدوار يبلغ نحو 2 طن من الاجهزة والمعدات فائقة التطور والحساسية حيث يبلغ طوله 9 امتار وسمكه نحو 1.8 متر، ناهيك عن مجموعة كبيرة من الكمبيوترات والأجهزة الالكترونية المتقدمة جدا التي توضع داخل جسم الطائرة. لذا فقد توجه الفريق العراقي بطلب من القيادة العراقية يفاتحها بحاجته للإطلاع على طائرة الاواكس الموجودة لدى المملكة العربية السعودية عدة نسخ منها، إلا ان الحكومة السعودية التي وافقت على الطلب العراقي شريطة عدم تفكيك اجهزة طائرة الاواكس، جعلت الفريق العراقي المكلف بتصنيع منظومة رادار الانذار المبكر امام خيار وحيد وهو الاعتماد على الذات لانجاز هذا المشروع العلمي قبل ان يكون مشروعا عسكريا يخدم اغراض الدفاع الجوي والحرب الالكترونية.

هكذا وعلى مدار 24 ساعة يوميا ولمدة ستة اشهر متواصلة , استمر الفريق العراقي من مهندسين وفنيين بالعمل على انجاز هذا المشروع الفائق التطور، حتى اضطر اعضاء الفريق العراقي المكلف بتصنيع منظومة الاواكس على النوم داخل الطائرة بدل الذهاب لبيوتهم. وبعد ستة أشهر من العمل المتواصل نجح الفريق العراقي بانجاز النموذج الاول من منظومة السيطرة والإنذار المبكر المحمولة جوا مع القرص الدوار الذي ركب على طائرة انتونوف 76 ، ولكن ما ان حلقت هذه الطائرة حتى سقطت، مما اجبر الفريق العراقي على اعادة حساباته من جديد، حيث نجح الفريق العراقي في منتصف عام 1989 من اجراء التجربة الناجحة الاولى للاواكس العراقية والتي سميت بطائرة عدنان – 1 اما كلفة الطائرة العراقية الواحدة من هذا الطراز فقد بلغت 26 مليون دولار فقط وهو ثمن زهيد مقارنة بثمن الطائرة الاسرائيلية التي بلغت كلفتها 70 مليون دولار.

لقد اعتمد الخبراء العراقيين في تصنيعهم لطائرة عدنان – 1 على رادار (TIGER) الفرنسي المنشأ ايضا والذي اصبح رادار محمول بلغ مداه 350 كم قادر على رصد مختلف انواع الاهداف الجوية المعادية ذات المقطع الراداري 2 متر مربع و بدقة تبلغ 80 % كما تم تزويدها بجهاز (IFF) بريطاني الصنع يسمح بالتعرف على الطائرات الصديقة من المعادية. وقد تم نقل طائرة عدنان الى ايران قبيل حرب عام 1991 ايضا وأصرت الحكومة الايرانية على عدم ارجاعها هي الاخرى للعراق حتى يومنا هذا، ويذكر ان هذه الطائرة قد سقطت اثناء مشاركتها لعرض جوي قامت به القوة الجوية الايرانية عام 2011.

لم يوقف الخبراء العراقيين جهودهم لتطوير منظومة السيطرة والإنذار المبكر المحمولة جوا رغبة منهم لزيادة مدى الكشف الراداري للأهداف الجوية المعادية، فقد تمكن الفريق العراقي في عام 1990 من تصنيع منظومة اخرى اكثر تطورا سميت بطائرة عدنان

وقد بلغ مدى الكشف الراداري لهذه الطائرة 450 كم حيث اعتمد الخبراء العراقيين على نسخة مطورة من الرادار الفرنسي وهو (TIGER-G) اما باقي المواصفات الفنية فهي ذاتها الموجودة في طائرة عدنان – 1.

وقد تم صنع منظومة واحدة فقط من طائرة عدنان – 2 تم تدميرها بإحدى غارات التحالف الدولي على قاعدة الحبانية الجوية خلال حرب عام 1991.

2- منظومة سراب للتشويش الالكتروني على الصواريخ المضادة للرادار :

قبيل نشوب حرب عام 1991، وبعد دراسة دقيقة لبطاريات صواريخ سام 3 / البيجورا قام بها فريق من الخبراء العراقيين المتخصصين في الدفاع الجوي والحرب الالكترونية، تم تصنيع هذه المنظومة التي وضعت بالقرب من بطرية صواريخ سام 3 / البيجورا تبث اشارات كهرومغناطيسية بنفس تردد الاشارات التي يرسلها رادار تلك البيطرية من اجل ابعاد صواريخ العدو وتشتيتها بعيدا عن اهدافها الحقيقة المتمثلة برادارات البيجورا. وقد تم تصنيع (80) وحدة من هذه المرسلات الكاذبة حيث حققت نجاحا كبيرا في استنزاف صواريخ العدو المضادة للرادار كصواريخ هارم (HARM) الاميركية وصواريخ الارم (ALARM) البريطانية.

المنظومة العراقية للتشويش على طائرة الاواكس (E-2C):

عقب حرب عام 1991، ومع توجه القيادة العراقية نحو الحفاظ على العنصر البشري والمادي للدفاع الجوي العراقي، فقد توجه الخبراء العراقيين نحو تصنيع منظومة اخرى خصصت للتشويش على طائرات الاواكس من طراز (E-2C) الداعمة لطائرات العدو الاخرى اثناء تحليقها في منطقتي حظر الطيران. وبالفعل فقد نجح الفريق العراقي المكلف بتلك المهمة من تصنيع منظومة تشويش قادرة على تهديد امن وسلامة طائرة الاواكس من طراز (E-2C).

كانت التجربة الاولى لهذه المنظومة في قضاء ابو الخصيب (14) كم جنوب مدينة البصرة، حيث تم وضع منظومة التشويش على شاحنة متنقلة وعندما دخلت الطائرة تم البدء بالتشويش عليها فشعرت الطائرة بخطر التشويش فانسحبت، وجاءت فورا الطائرات المقاتلة لتقصف المنطقة ولكن المنظومة كانت قد تمكنت من مغادرتها بسلام.

بعد التجربة الناجحة التي اجرتها منظومة التشويش العراقية ضد طائرات الاواكس، فقد وجهت القيادة العراقية بتصنيع اعداد اخرى بغية تامين حاجة جميع مناطق جنوب العراق من هذه المنظومة. فوجد مسؤولي وزارة الدفاع الامريكية البنتاغون انفسهم مرغمين على سحب جميع طائرات الاواكس (E-2C) ولم تقم بعدها بالطيران في منطقة حظر الطيران جنوب خط عرض 33، وهكذا فقد سجلت هذه العملية كواحدة من افضل الانجازات العراقية في الحرب الالكترونية.

منظومة التحكم والسيطرة على طائرة بريداتور :

بعد ان قطع البحث العلمي العراقي مرحلة متقدمة جداً في التكنولوجيا الالكترونية عموما وفي تقنيات الميكروويف المتطورة خصوصا، فقد اصدرت القيادة العراقية اوامرها لتنفيذ عملية خاصة ذات بعد سياسي وعسكري وتقني كبير شكلت احدى اكبر واهم المفاجئات التي نزلت كالصاعقة على مسؤولي البيت الابيض ووزارة الدفاع الامريكية البنتاغون.

فقد قام الخبراء العراقيين في الحرب الالكترونية بابتكار منظومة متطورة تعتمد على تقنية موجات الميكروويف عالية الكثافة شديدة القصر HDM.Microwaves.High.Density)) مكنتهم من السيطرة والتحكم بطائرة التجسس الامريكية بريداتور (RQ.1B. Predator) ذات التكنولوجيا الفائقة التطور والمسيرة عن بعد 600 كم، حيث نجح الخبراء العراقيين في الدخول على نظام توجيه هذه الطائرة والتحكم بها ومن ثم إنزالها على مدرج مطار في شمال العراق في حدود الساعة التاسعة والنصف من صباح يوم الاحد 5/26 /2002 وهي في حالة سليمة تماما وبدون ان تصاب بخدش واحد.

وهو الانجاز الذي سبق فيه العراق جميع بلدان العالم ومكنه من اكتشاف واحدة من اكثر اسرار التكنولوجيا الامريكية فائقة التطور، كما نجح العراق في اسقاط عشرات الطائرات الاستطلاعية الامريكية مسيرة عن بعد، كانت حصة الاسد من نصيب طائرة البريداتور وهي احدث طائرة تجسس من دون طيار تفتخر الادارة الامريكية بصناعتها.

وبعد محاولات كثيرة استغرقت عدة اشهر من البحث عن المستند الاخباري لهذا الحدث العظيم الذي جرى التعتيم عليها منذ لحظة حدوثه وحتى يومنا هذا، تمكنا من التوصل الى الموقع الوحيد الذي انفرد بنشره يوم 2002/5/27 وهو موقع البوابة تحت عنوان (العراق يسيطر على طائرة تجسس اميركية) وفيما يلي نص الخبر :

اكد العراق اليوم الاثنين 2002/5/27 انه تمكن من السيطرة على طائرة من دون طيار يعتقد انها اميركية، وذلك خلال قيامها بمهمة تجسس في شمال العراق امس الاحد حيث قادها الى الهبوط في الاراضي العراقية.

ونقلت وكالة الانباء العراقية عن ناطق باسم قيادة الدفاع الجوى قوله انه "في الساعة 9.30 بالتوقيت المحلي (5,30بتوقيت غرنتش) من 26 ايار/ مايو الجاري اخترقت حرمة الاجواء العراقية طائرة بدون طيار في المنطقة الشمالية من قطرنا العظيم للقيام بأعمال تجسسية عدوانية. وتم رصد الطائرة من قبل وسائل دفاعنا الجوى والسيطرة عليها بوسائلنا الخاصة وإجبارها على الهبوط داخل اراضينا".

وقال الناطق العراقي "بذلك يؤكد مقاتلو الدفاع الجوى قدرتهم على مواجهة اساليب العدو التجسسية لاستخدام كافة وسائله ذات التقنية العالية والمتطورة للحصول على المعلومات لإسناد طائراته المقاتلة للقيام بالعدوان على منشاتنا الحيوية والخدمية وممتلكات المواطنين".

وجاء الاعلام عن السيطرة على هذه الطائرة المسيرة بعد التقارير التي تحدثت يوم امس عن سقوط طائرة اميركية مسيرة بدون طيار في المنطقة الجنوبية من العراق. يذكر ان الدفاعات الجوية العراقية اعلنت خلال الاشهر الماضية عن اسقاط ثلاث طائرات من دون طيار كانت تقوم بطلعات تجسسية فوق جنوبي العراق في منطقة حظر الطيران.

واعترفت واشنطن بأنها فقدت ثلاثا من طائراتها في 10 تشرين الاول/اكتوبر و 11 ايلول / سبتمبر و 27 اب / اغسطس 2001 بحسب بغداد. وكانت سقطت في الكويت السبت الماضي (2002/5/25) طائرة تجسس اميركية من دون طيار لدى عودتها من "مهمة استطلاع". يشار الى ان مواجهات شبه يومية تدور بين العراق والطيران الاميركي والبريطاني الذي يتولى مراقبة منطقتي الحظر الجوي في شمال العراق وجنوبه. ولا تعترف بغداد بمنطقتي الحظر الجوي اللتين لم يصدر بشأنهما اي قرار دولي.)) انتهى نص الخبر.

كما نشرت شبكة بي بي سي الاخبارية البريطانية على موقعها الالكتروني في الانترنت يوم 2002/12/24، خبرا عن قيام الدفاع الجوي العراقي بإسقاط طائرة بريداتور، جاء فيه :

أبرزت كافة الصحف البريطانية الرئيسية الصادرة صباح الثلاثاء 24 ديسمبر/ كانون الاول نبأ اسقاط العراق لطائرة تجسس أمريكية بدون طيار من طراز "بريداتور" جنوبي منطقة حظر الطيران.

وتقول صحيفة الاندبندنت إن إسقاط الطائرة هو الحادث الأول من نوعه منذ صدور قرار مجلس الأمن رقم 1441 بخصوص عمليات التفتيش على أسلحة الدمار الشامل في العراق والذي عاد بمقتضاه المفتشون الى بغداد وقالت الصحيفة إن رئيس هيئة الاركان المشتركة في الجيش الامريكي "ريتشار مايرز" أكد نبأ إسقاط الطائرة. ونقلت الصحيفة عن "مايرز" قوله "إن القوات العراقية حالفها الحظ وأسقطوا البريديتور".

كما نقلت الصحيفة عن متحدث عسكري عراقي قوله "بعون من الله وبعزيمة الأبطال من رجال قوات الدفاع الجوي ونسور الجو الشجعان وفي عملية دقيقة مخططة تم إسقاط الطائرة". وتضيف الصحيفة أن الحادث أثار حالة من القلق حيث إن كافة الهجمات التي كانت تستهدف المقاتلات الأمريكية والبريطانية من قبل كانت تتم من خلال صواريخ أرض جو تطلقها الدفاعات العراقية وليس عن طريق الطائرات الحربية العراقية. وتعدد الصحيفة في هذا الصدد العمليات السابقة ومن بينها إعلان العراق في اكتوبر/ تشرين الأول من عام 2001 عن اسقاط طائرة من نفس الطراز وكذلك نجاحه في اجبار طائرة دعم جوي أمريكية بدون طيار على الهبوط في مايو/ آيار الماضي.2002

أما صحيفة الديلي تلجراف فتتحدث ببعض التفصيل عن كيفية إسقاط الطائرة. وتقول الصحيفة إن طائرة عراقية من طراز ميج 29 على الارجح اخترقت منطقة حظر الطيران الجنوبية في الساعة 12.35 بتوقيت جرينتش وقامت بإطلاق صاروخ على الطائرة الأمريكية التي كانت قد انطلقت في وقت سابق من قاعدة بالكويت مما أدى الى سقوطها مشيرة إلى أنه لم يتمكن من رصد

حطام الطائرة الى هذه اللحظة. ونقلت الصحيفة عن متحدث عراقي قوله إن الطائرة انتهكت السيادة الجوية العراقية ولذلك تم اسقاطها. وتشير الصحيفة الى أن الطائرة من طراز بريديتور تجهز عادة بصواريخ موجهة بالليزر وهو نفس النوع الذي استخدمته وكالة الاستخبارات المركزية الامريكية بدقة كبيرة في أفغانستان وكذلك في اغتيال قائد سليم سنان الحارثي وخمسة آخرين من منظمة القاعدة في اليمن الشهر قبل الماضي. وتضيف الصحيفة ان تكلفة الطائرة من هذا الطراز تصل الى 2.6 مليون دولار وكانت قد اشتركت لأول مرة في المعارك الحربية أثناء حرب البوسنة عام 1995 عندما استخدمت في رصد مواقع المدفعية الصربية مشيرة الى أنه جرى تطويرها بعد ذلك لتتحول الى آداة حربية قاتلة يمكن التحكم فيها عن بعد يصل الى 400 ميل / 600 كم.

من جانبها، تناولت صحيفة الجارديان أحدث الانشطة التي بدأها المفتشون التابعون للأمم المتحدة الموجودون بالعراق حاليا. وقالت الصحيفة إن المفتشين الدوليين بدؤوا مرحلة جديدة في عملياتهم بالبدء في استجواب العلماء العراقيين على أمل تقديمهم أدلة على وجود اسلحة بيولوجية او نووية او كيماوية وهو ما ستعتبره إدارة الرئيس بوش سببا لبدء الحرب. ونقلت الصحيفة عن محمد البرادعي رئيس الوكالة الدولية للطاقة النووية قوله:" إن المفتشين التابعين للوكالة بدؤوا حاليا عملية استجواب أفراد داخل العراق على انفراد"، ولكنه أضاف أنهم لم يتوصلوا بعد الى الكيفية التي يمكن بها استجواب هؤلاء العلماء مشيرا الى ضرورة تامين هؤلاء العلماء اولا او اعطائهم حق اللجوء السياسي

حيث إنهم يخشون على سلامتهم وسلامة أسرهم في العراق إذا ما أدلوا بأي معلومات.

وأخيرا وتحت عنوان يتسآل "لماذا ستنتهي أي حرب ضد العراق كلمح بالبصر" عرضت صحيفة التايمز تصورها للمسار الذي ستأخذه الحرب المنتظرة ضد العراق والتي ستنتهي في عشرة أيام وفقا لتصور الصحيفة. وفي هذا الصدد تقول الصحيفة إن الولايات المتحدة تعتزم جعل حربها ضد العراق واحدة من أسرع العمليات العسكرية التي نفذت حتى الآن باستخدام أسلحة سرية جديدة للقضاء على أي مقاومة عراقية والإطاحة بصدام حسين. ومن بين الأسلحة التي عرضت لها الصحيفة الصواريخ من طراز "إيدام" ذات القوة التدميرية الكاسحة وصواريخ "جيسو" التي ستستهدف الرادارات العراقية والقنابل الحرارية التي تتولد عنها درجة حرارة وضغط هائلين بالإضافة الى الطائرات من طراز "بي 2 ستيلث " او الشبح وطائرات اف 18 والطائرات من طراز بريديتور (التي أسقط العراق احدها بالأمس). كما تعرض الصحيفة لما يطلق عليه "قنبلة الميكرويف" التي سيكون بمقدورها قطع التيار الكهربي عن العاصمة العراقية بأسرها دون تدمير أي مبنى.

وتضيف الصحيفة أن واشنطن نجحت في فرض سيطرتها على الاجواء العراقية بشكل كبير من خلال شبكة من الصواريخ الموجهة عن طريق الأقمار الصناعية وهو ما سيؤدي الى تدمير مئات المواقع العراقية في أول ليلة فقط من العمليات العسكرية.

منظومة السيطرة والتحكم بالذخائر المنزلقة على الليزر :

تمكـن الخـبراء العـراقيين في الحـرب الالكترونيـة وبمـساعدة خارجيـة محـدودة في أواسـط التسعينات، من ابتكـار منظومـة متطـورة تـستخدم تقنيـة الليـزر فائقـة التقـدم للـسيطرة والتحكم بذخائر العدو المنزلقـة عـلى الليـزر ((LGB والمعروفـة ايـضا بقـذائف البيـف وي (Pave.Way). وطالما كان في مقدور المنظومة العراقية، القدرة على السيطرة والتحكم بهذه الانواع من ذخائر العدو، فقد كان بمقدورها ايضا تضليل تلك الاسلحة نحو اهـداف وهميـة او توجيهها نحو صفوف العدو نفسه.

تتكون المنظومة العراقية للسيطرة والتحكم بـذخائر العـدو المنزلقـة عـلى الليـزر وبحـسب فهمنا لما جاء في مقالة الاخ العزيز محب المجاهدين المنشورة تحت عنوان (الأمن الخـاص و الحرب الخفية في الفلوجة) بتاريخ 2004/8/22، من عدة أجهزة تولـد حـزم ليزريـة مـشفرة بكود عراقي سري ومخروطية الشكل حيـث يكـون رأسـها عـلى جهـاز ارسـال اشـعة الليـزر المركب في المنظومة العراقية نفسها، بينما تكون قاعـدة المخـروط في الـسماء ليتـسنى لهـذه المنظومة السيطرة والتحكم على اكثر عدد ممكن من ذخائر العدو المنزلقة على الليزر.

يـتم ضـبط تـردد الحـزم الليـزر التـي تطلقهـا المنظومـة العراقيـة، بـنفس تـردد الحـزم الليزريــة التــي تولــدها الطــائرات المعاديــة، ولكــن بــشفرة سريــة عراقيــة خاصــة. حيــث يقــوم معــالج الكــتروني عــالي الــسرعة فــائق التقنيــة، متــصل بجهــاز لاقــط متطــور للغايــة، بالتقــاط وضــبط النطــاق الــترددي للحــزم الليزريــة التــي تولــدها الطـائرات المعاديـة وتطلـق ذخائرهـا عليهـا، كـما يقـوم المعـالج الالكـتروني الموجـود في

المنظومة العراقية في الوقت نفسه بفك شفرة الحزم الليزرية المعادية ثم يقوم في الوقت عينه بتشفير الحزم الليزرية العراقية والتي يتم التحكم بانعكاسها من على عدة اهداف وهمية الامر الذي يشكل نقطة تهديف وهمية تنزلق نحوها قذائف العدو الذكية بدل حزم الليزر التي ولدتها الطائرات المعادية، وبهذه الالية تتمكن المنظومة العراقية من السيطرة على الذخائر المعادية بدون ان يشعر العدو، ومن دون ان تخرج ذخائره المنزلقة على الليزر عن حزم الليزر الموجهة لها.

مع العلم ان باستطاعة المنظومة العراقية ومن خلال تحكمها بانعكاس اشعتها الليزرية، اختيار أي بقعة لتكون نقطة تجمع الاشعة والتي ستكون كنقطة تهديف وهمية تضل ذخائر العدو المنزلقة على الليزر

منظومتي السيطرة والتحكم على الذخائر الموجهة بالأقمار الصناعية :

طور الخبراء العراقيين في الحرب الالكترونية منظومتين للسيطرة والتحكم بذخائر العدو الموجهة بالأقمار الصناعية من فئة قذائف الهجوم المباشر المشتركة (JADM) التي تطلقها الطائرات من على مسافة 28 كم، اما الفئة الاخرى للذخائر الموجهة بالأقمار الصناعية فهي الصواريخ الجوالة من طراز كروز توماهوك (Cruise.Tomahawk). كما قامت القيادة العراقية باستيراد محطات وأجهزة تشويش على الاقمار الصناعية الامريكية، وقد تناقلت وكالات الانباء والصحافة العربية والعالمية الاخبار التي تحدثت عن سعي العراق للحصول على هذه المعدات المتطورة.

فمن الجدير ذكره هنا وهو ما قد يفاجئ جميع قرائنـا الكـرام، ان قـذائف الهجـوم المبـاشر المشتركة (JADM) التـي اسـتغرقت شركـات امريكيـة عريقـة سـنوات عديـدة في تطويرهـا وتفـاخرت بهـا الادارة الامريكيـة، كانـت مبعـث قلـق كبـير لخـبراء وزارة الـدفاع الامريكيـة البنتاغون التي لم تهنئ بقذائفها الذكية. فلم يمر 30 يوماً عن إعلان وزارة الـدفاع الامريكيـة يوم 1998/2/11 عن نجاح خبراء شركة بوينغ لصناعة الطائرات وهي احـدى اكبر الـشركات الـصناعية المتقدمـة في الولايـات المتحـدة الامريكيـة في اجـراء اول تجربـة ناجحـة لقـذائف الهجوم المباشر المشتركة (JADM) موجهـة بـالأقمار الـصناعية، إلا وتبـين لوكالـة المخـابرات المركزية الأمريكية السي أي ايه ان لدى العراق القدرة على تضليل قذائف البنتاغون الذكية.

ومنذ يونيو حزيران عام 2002 والإدارة الامريكية تحتج على الحكومة الروسية التي اتهمتهـا بتزويد العراق بمعدات وأجهزة عسكرية متطورة، منها اجهزة تشويش على الاقمار الصناعية الامريكية. كما ادعت السي أي ايه بان في حوزة القيادة العراقية نحو (2400) جهاز تشويش على الاقمار الصناعية الامريكية كانت قد استوردتها من روسـيا الاتحاديـة. وعرضـت شـبكة فوكس الاخبارية الفـضائية الامريكيـة صـورا قالـت عنهـا الــ(CIA) انهـا اجهـزة التـشويش الروسية التي يمتلكها العراق، كما عرضت خرائط باللغـة الروسـية توضـح أمـاكن الـرادارات التى تسعى المقاتلات الأمريكية إلى تدميرها فى الضربات الجوية الافتتاحية للحرب.

وفي خـبر مثـير للـسخرية ذا صـلة، فقـد صرح أحـد المـسؤولين الأمـريكيين أنـه في حـال تحويـل القنابـل الذكيـة عـن أهـدافها، فـإن لا أحـداً سـيعرف أيـن سـتسقط ولا مـن

ستصيب، وأسوأ الاحتمالات هنا أن تسقط فوق مناطق مدنية وتودى بحياة المدنيين وهو ما يستطيع صدام حسين استغلاله لإحراج القوات الأمريكية فى إطار استراتيجيته المعروفة بالأرض المحروقة. لذلك يتوقع أن تواجه القيادة الامريكية هذه المشكلة بأسلوبين، الأول انزال قوات امريكية خاصة او استمالة قوات عراقية للانقلاب ضد القيادة العراقية تقوم بتحديد مواقع الرادارات العراقية لاسيما القريبة من المناطق السكنية، او تبعا للأسلوب الثانى وهو إدخال تحسينات على نظام توجيه القنابل الذكية بحيث لا تتأثر بالتشويش الرادارى الروسى.

هكذا ولخمسة سنوات اخرى وعلى ذات المنوال استمرت الادارة الامريكية في حملتها الاعلامية لتشويه الانجاز العراقي وشاركتها للأسف الشديد وسائل اعلام عربية . اما بالنسبة لموقف القيادة العراقية من قذائف البنتاغون الذكية، فقد كانت محط سخرية لها، حيث اعلنت الصحف العراقية عن نجاح الخبراء العراقيين بتصنيع منظومة تشويش خاصة على الاسلحة الامريكية الذكية والتي ستحيلها الى مجرد اكوام من حديد السكراب كما عبر عنها حينذاك الرئيس صدام حسين.

يجدر بالإشارة ان 80 % من القذائف والصواريخ التي تعتزم الادارة الامريكية استخدامها في حربها لغزو العراق تعتمد على التوجيه بالأقمار الصناعية الامر الذي يوضح مدى خطورة الاوضاع بالنسبة للقوات الامريكية فيما لو صحت الانباء عن امتلاك القيادة العراقية لأجهزة متطورة باستطاعتها التشويش على الاقمار الصناعية التي تستخدمها وزارة الدفاع الامريكية لتوجيه قذائفها الذكية.

وهنا نود ان نبين للقراء الكرام ومن خلال متابعتنا للإخبار التي تحدثت عن اجهزة التشويش التي بحوزة العراق، فقد تمكنا من التعرف على حقيقة الادعاءات الامريكية عن قيام العراق باستيراد اجهزة تشويش روسية الصنع. فعلى ما يبدو فان القيادة العراقية قامت قبل الحرب بعقد صفقة سرية مع روسيا الاتحادية تعمدت تسريب بعض تفاصيلها لاستيراد محطات تشويش ثابتة – وليس اجهزة تشويش. وفي عام 1998 وباحدى زياراته للعراق قام فلاديمير جيرينوفسكى زعيم الحزب الليبرالي الديمقراطي الروسي بتزويد القيادة العراقية بجهازي تشويش على الاقمار الصناعية الامريكية حصل عليهما من شركة تدير العمليات التسويقية لمنتجات جامعة ولاية تشيلابينسك (Chelyabinsk.university) الروسية من تصميم احد علماء قسم انظمة التوجيه والسيطرة في الجامعة المذكورة. وعلى اثر التجارب التي قام بها الخبراء العراقيين على جهازي تشيلابينسك ونجاحهما في التشويش على الاقمار الصناعية الامريكية، فقد قامت القيادة العراقية باستيراد مابين 40 الى 45 جهاز تشويش اخر.

وفي يوليو تموز عام 2000، تحدثت صحيفة القبس الكويتية عناجهزة التشويش على الاقمار الصناعية الامريكية التي بحوزة العراق، وقد نشرت وكالةالانباء الكويتية "كونا" الخبر المذكور في موقعها الرسمي على الانترنتيوم 2000/7/16، حيث جاء فيه :

((كشفت صحيفة (القبس) الكويتية فى تقرير لها اليوم تفاصيل حصول العراق على جهاز تشويش روسى يمكنه التأثير على اجهزة التوجيه التى تستخدمها

الاقمار الصناعية الامريكية داحضة الاكاذيب التى زعمت ان العراق تمكن من اكتشاف جهاز يحول الصواريخ الامريكية الى "حديد خردة".

واستعرضت صحيفة (القبس) فى تقريرها من موسكو تفاصيل زيارة مراسليها الى مدينة تشيلابينسك الروسية المعروفة منذ العهد السوفيتى بأنها تحتوى على اهم مجمع نووي تكنولوجى وعسكرى فى الاتحاد السوفيتى السابق. ودحضت الصحيفة بالأدلة والصور الاكاذيب التى نشرتها الصحف العراقية والتى كانت تزعم ان القدرة العراقية نجحت فى التوصل الى جهاز يمكنه افشال الصواريخ الامريكية وان كل ذلك تم بتوجيهات من رئيس النظام العراقى صدام حسين على حد زعمها.

وأجرت (القبس) لقاءات مع علماء احدى جامعات مدينة تشيلابينسك العريقة شرحوا فيها كيفية عمل الجهاز والوسيلة التى حصل عليها العراق على نماذج منه. وكان قسم انظمة التوجيه والسيطرة التابع للجامعة قد توصل بجهود احد المختصين بالعلوم التكنولوجية الى اختراع جهاز يلغى تأثير نظام (جى بى اس) المعمول به فى الاقمار الصناعية الامريكية. وذكر المختص الذى رفض ذكر اسمه للقبس ان اختراعه سيكلف الامريكيين خسارة لأتقل عن 100 مليار دولار مؤكدا ان " بإمكان جهازه تحويل كل الاقمار الامريكية الى حديد بلا فاعلية تماما كما قال صدام حسين الذى سمع العبارة وحفظها دون فهم على الارجح".

وأشارت (القبس) الى كيفية حصول العراق على جهازين من هذا النوع عن طريق الزعيم القومى الروسى فلاديمير جيرينوفسكى الذى ادرك حاجة العراق الماسة فى هذا الوقت لعمل شيء ما للطائرات الامريكية والبريطانية التى

تفرض الرقابة على مناطق حظر الطيران الجوى. وكان جيرينوفسكى قد حصل بدوره على هذين الجهازين من شركة وسيطة فى موسكو تتولى تسويق انتاج الجامعة المذكورة ويقتصر عملها على الوساطة والسمسرة فى صفقات السلاح ولا تملك اى شيء غير ذلك بالرغم من انها تعلن نفسها مصنعة لكل الاجهزة والمعدات التى تتاجر بها.

ونقلت صحيفة (القبس) عن علماء الجامعة المعنية قولهم ان جهاز التشويش السهل الحمل والصغير الحجم سعر المفرد فى حالة بيعه من الجامعة مباشرة يساوى 18 الف دولار ويصل سعره الى 8 آلاف دولار فى حالة شراء 100 جهاز او اكثر بينما تبيعه الشركة الوسيطة بمبلغ 50 الف دولار وهى تقوم فقط بنقله من تشيلابينسك الى موسكو.

وأشار هؤلاء العلماء الى ان الظروف دفعت قيادة الجامعة الى البحث بنفسها عن زبائن عن طريق المؤسسة التجارية التابعة لها وبدأت بمخاطبة قيادات الدول التى توجه لها الضربات مثل العراق ويوغسلافيا او المرشحة لتلقى هذه الضربات.

وأوضحت الصحيفة ان العراق حصل على مابين 40 و 45 جهازا وبعد ان اجرى التجارب عليه، قرر صدام اعلان خبر توصل الخبراء العراقيين الى طريقة يعمون بها الصواريخ الامريكية ويحولونها الى حديد خردة بناء على توجيهات صدام.

ونسبت (القبس) الى مصادر مطلعة قولها ان الشركة الوسيطة فى موسكو التى قيل انها اشترت حق بيع هذا الجهاز لم تعلم بعمليات تهريب الجهاز الى العراق وهذا يعنى ان الحكومة الروسية قد لا تعلم بهذا الامر. وذكر المختص الروسى (للقبس) ان العراق خسر الحرب مع الحلفاء بفضل الاشارات الراديوية التى كانت الاقمار الصناعية الامريكية ترسلها بواسطة نظام (جلوبال بوزيشونينغ سيستم) الذى يمكن لأي مستقبل ومرسل معرفة المعطيات المطلوبة لأي هدف على الارض او فى الجو او البحر. وأضاف قائلا كان علينا ان " نشل قدرة هذا النظام بتوجيه حزم راديوية ذات اطوال موجية عالية تشوش عمله وتفقد اتصاله مع الطائرات والصواريخ المجنحة فى مدى عمل الجهاز وعندها يتم التعامل مع الصاروخ او الطائرة المهاجمة بشكل تقليدى بعد ان فقدت هدفها المسيطر عليه من الاقمار الصناعية".

وقالت الصحيفة انه يمكن وضع الجهاز وتشغيله بمجهز قدرة عادى فى المواقع الحكومية والمجمعات المهمة ويمكن تغطية بلد بأكمله فى حالة توفر عدد كبير من الاجهزة يتناسب مع اراضى ذلك البلد. ونقلت (القبس) عن المختص الروسى قوله ان جهازه سيؤدى الى الحاق خسائر مادية كبيرة للأمريكيين مشيرا الى ان هذه المبالغ ستصرف على تعديل منظومة (جى بى اس). وذكر انه فى حال تمكن الولايات المتحدة من اجراء التغييرات اللازمة على النظام نفسه فان العلماء الروس سيلحقون بهذه التغييرات وسيتمكنون من كشفها وتصنيع جهاز مضاد لا يختلف من النواحى الاستاتيكية عن السابق سوى بتحويرات بسيطة.

وفي يناير كانون الثاني عام 2003 نشرت شبكة فوكس نيوز الاخبارية الامريكية خبرا عن حصول العراق على نحو (400) جهاز إلكتروني روسي الصنع قادر من خلال التشويش على الاقمار الصناعية الامريكية من التحكم بذخائر الهجوم المباشر المشترك (JADM)، وتضيف الشبكة الاخبارية موضحة بان لدى الادارة الامريكية شكوكا بان تلك الاجهزة تم ادخالها الى العراق في حاويات حجم 3 قدم مكعب على انها مساعدات انسانية للشعب العراقي.

وفي اثناء الغزو الامريكي للعراق في مارس اذار عام 2003 حدثت العديد من الحالات الغريبة، ففي يوم 2003/3/23 مثلا انطلق صاروخ باتريوت امريكي نحو طائرة تورنادو تابعة لسلاح الجو البريطاني عن طريق الخطأ ما أدى إلى مقتل طياريها الاثنين.

وبنفس ذلك اليوم اعلنت الولايات المتحدة الامريكية عن امتلاكها أدلة دامغة تثبت قيام روسيا الاتحادية بتزويد العراق بأسلحة ومعدات متطورة من بينها اجهزة تشويش على الاقمار الصناعية الامريكية. حيث اتهمت الادارة الامريكية الحكومة الروسية بتعاونها مع العراق وتزويده بمنظومة تشويش على اجهزة الرادار الموجودة في الطائرات الامريكية، وهو الامر الذي نفته وزارة الخارجية الروسية.

وقد نقلت شبكة فوكس نيوز الاخبارية الامريكية يوم 2003/3/23 عن قيام تجار روس بتزويد العراق بمعدات الكترونية وأسلحة متطورة، من بينها مئات الاجهزة لتشويش على الاقمار الصناعية وكميات كبيرة جدا من صواريخ مضادة

للدبابات منها صواريخ كورنت المتطورة والموجهة بالليزر، بالإضافة الى الالاف المناظير الليلية المتطورة، كما ادعت الشبكة المذكورة عن انتقال خبراء روس عسكريين الى العراق ابتدأ من يوم الجمعة 2003/3/21 لغرض تعريف الخبراء العراقيين بكيفية استخدام وصيانة المعدات والأسلحة المتطورة.

كما نشرت وكالة الانباء الكويتية "كونا" يوم 2003/3/24، خبرا حول تصريحات الادارة الامريكية، جاء فيه :

اكد البيت الابيض الامريكي اليوم وجود ادلة دامغة على ان روسيا باعت العراق معدات عسكرية متطورة منها مناظير ليلية وأسلحة مضادة للدبابات ومعدات تشويش على الذخائر التي توجهها الاقمار الصناعية.

ووصف المتحدث باسم البيت الابيض "آيري فلايتشر" في ايجاز صحافي تلك الاعمال بأنها "مزعجة" وقال انه تم ابلاغ السلطات العليا في موسكو باعتراض واشنطن عليها. كما شكك المتحدث بالمشاهد التي عرضها التلفزيون العراقي وتظهر ما يبدو انه تسجيل حديث لثاني خطاب يلقيه الرئيس العراقي صدام حسين منذ بدء الحرب الخميس الماضي. وقال في هذا الشأن " قد تكون تلك المشاهد صورت في وقت سابق قبل بدء المعارك". وأشار الى ان من الممكن بسهولة ان يعد صدام "بضع تصريحات مسبقا" على ان تذاع لاحقا.

من جانب آخر اعلن المتحدث باسم البيت الابيض ان الرئيس الامريكي جورج بوش سيزور مقر القيادة المركزية "سينت كوم" في مدينة تامبا بولاية فلوريدا الامريكية من اجل اظهار دعمه ومساندته للقادة العسكريين. وقال ان الرئيس

بوش سيتناول طعام الغداء في القاعدة ويمضي بعض الوقت مع قادة التحالف العاملين هناك

ولم تتوقف تصريحات الادارة الامريكية عند هذا الحد فحسب، بل ذهبت الى ابعد من ذلك، حيث اعلن احد المسؤولين الامريكان عن ان التشويش العراقي على الأقمار الصناعية يتم بأياد روسية، وقد اشار صحيفة الرياض السعودية في عددها (12694) الصادر بتاريخ الاثنين 2003/3/24، الى التصريح الامريكي، وفيما يلي نص الخبر :

((أفاد مسؤول أمريكي رفيع المستوى طلب عدم الكشف عن هويته ان الولايات المتحدة تظن ان فنيين روساً يساعدون العراق على تشويش بث عبر الأقمار الاصطناعية يعتبر اساسيا لتوجيه القنابل والطائرات الأمريكية والبريطانية.))

وفي يوم 2003/3/25 اعترف " ستانلي ماكريستال" قائد العمليات الخاصة المشتركة بان العراق استطاع عبر استخدامه لمعدات الكترونية متطورة روسية الصنع من التشويش على الاقمار الصناعية الامر الذي حيد الاسلحة المستخدمة في القتال كالطائرات والصواريخ. ويذكر ان القيادة العامة للقوات المسلحة العراقية كانت قد اعلنت في بيانها السادس من تمكن الدفاعات الجوية العراقية في ذلك اليوم من اسقاط نحو (122) صاروخا جوال من طراز كروز.

واستمرت الولايات المتحدة الامريكية تتحدث عن اجهزة التشويش التي بحوزة العراق حتى بعد غزوها له، حيث نشرت صحيفة الشرق الاوسط في عددها

(9175) الصادر يوم الاحد 2004/1/11 خبرا تحت عنوان "واشنطن : لدينا ما يثبت بيع روسيا أسلحة لصدام استخدمت في الحرب الأخيرة " جاء فيه :

واشنطن «الشرق الأوسط» : عثر مسؤولون اميركيون على أدلة تؤيد مزاعم الادارة بأن الشركات الروسية باعت للرئيس العراقي المخلوع صدام حسين معدات عسكرية متطورة هددت القوات الاميركية خلال غزوها العراق في مارس (آذار) 2003.

وأضاف المسؤول ان الولايات المتحدة وجدت ادلة تشير الى ان الشركات الروسية باعت للعراق نظارات للرؤية الليلية ومعدات للتشويش على الرادار. وتتضمن الادلة المعدات ذاتها وما يدل على استخدامها اثناء الحرب الاخيرة. وإذا تأكد ذلك، فان روسيا تكون قد انتهكت عقوبات الامم المتحدة على العراق. ونسبت صحيفة «لوس انجليس تايمز» الى المسؤول قوله «لقد تأكدنا من بعض الادلة». وأضاف المسؤول ان واشنطن لم تتلق اطلاقا تفسيرا من روسيا يهدئ مخاوفها، وان القضية بالتالي وإن حصلت في الماضي «ما زالت حساسة بالنسبة للعلاقات». وتابع «يمكن ان نقول ان القضية لم تعزز بناء الثقة».

وأثيرت القضية في البداية في 24 مارس الماضي اي بعد اندلاع الحرب بأيام عندما اتصل الرئيس الاميركي جورج بوش بنظيره الروسي فلاديمير بوتين ليعرب عن قلقه حيال اجهزة الرؤية الليلية ومعدات التشويش على الرادار ومنظومات صاروخية مضادة للدبابات روسية، كانت تستخدم من قبل قوات صدام حسين.

اما بالنسبة للأخ العزيز محب المجاهدين، فلم تكن قضية استيراد العراق لأجهزة التـشويش ليغيب عن مواضيعه، حيث ذكر في مقالتـه المعنونـة (مـن الـذي خـان العـراق) والمنـشورة بتاريخ فجر 2006/1/2، بان القيـادة العراقيـة قامـت باسـتيراد محطـات تـشويش وتـضليل للإشارة التـي يعتمـد عليهـا نظـام تحديـد المواقـع العـالمي (GPS) التـابع لمجموعـة اقـمار "نافستار" العائدة لوزارة الدفاع الامريكية. ولكن فقد كان لمحطات التشويش الروسية نقطة ضعف واضحة، حيث يخبرنا محب المجاهدين بأن تلك المحطـات كـان يجـب ان توضـع في مباني كونكريتية ثابتة، الامر الذي حال دون امكانية نقلها بالعربـات والعجـلات العـسكرية كما هو الحـال بالنـسبة مـع أنظمـة البـث التلفزيـوني العراقـي او حملهـا مـن قبـل رجـال العمليات الخاصة مـما جعلهـا هـدفاً سـهلاً لطـائرات المهـمات الجراحيـة الأمريكيـة أمثـال "ستلس فايتر" والبريطانية من فئة تورنادو.

ومن خلال متابعتنا لمقالات الاخ محب المجاهدين فقد توصـلنا لـبعض تفاصـيل منظـومتي التـشويش عـلى الـذخائر الموجهـة بـالاقمار الـصناعية اللتـان نجـح الخـبراء العـراقيين مـن تصنيعهما داخل العراق، وهما :

أ - منظومة الامواج الفوق صوتية للسيطرة والتحكم على الذخائر الموجهة بالأقمار الصناعية :

تعمل هذه المنظومة وفق نفس الالية التي تعمل عليهـا منظومـة الـسيطرة والـتحكم عـلى الـذخائر المنزلقـة عـلى الليـزر، ولكـن بـدلا مـن اعتمادهـا عـلى اجهـزة تولـد حـزم ليزريـة فـان اجهـزة هــذه المنظومــة تولــد حــزم مــن الموجــات الفــوق صــوتية كتلــك التــي

يعتمد عليها نظام تحديد المواقع العالمي (GPS) التابع لمجموعة اقمار "نافستار" العائدة لوزارة الدفاع الامريكية.

حيث يقوم المعالج الالكتروني الفائق السرعة الموجود في المنظومة العراقية وعبر جهاز لاقط متطور بضبط النطاق الترددي للموجات الفوق صوتية التي تولدها مجموعة اقمار نافستار، ويقوم بذات الوقت بفك شفرتها، ثم يتبعها وخلال اجزاء قليلا جدا من الثانية بإرسال موجات فوق صوتية بنفس تردد الموجات الامريكية ولكن بشفرة عراقية خاصة تضلل مجموعة أقمار نافستار الامريكية حيث تنعكس الموجات العراقية على عدد من الاهداف الوهمية مما يشكل نقطة تهديف وهمية عند الاقمار الامريكية التي تقوم بإرسال قذائف الهجوم المباشر المشتركة (JADM) التي تطلقها الطائرات وصواريخ كروز توماهوك (Cruise.Tomahawk) الجوالة نحوها اي نحو الهدف الوهمي.

صواريخ كروز توماهوك (Cruise.Tomahawk) الجوالة التي زودت بعض انواعها بتقنية التوجيه عبر الاقمار الصناعية

مع العلم ان بقدرة المنظومة العراقية تحديد النقطة الوهمية حيثما تريد والتي غالبا ما تكون فوق اقرب هدف معادي اي نحو القوات الامريكية ذاتها وبهذه الالية المتطورة تمكنت قوات خاصة عراقية قبل الغزو وبعده من تدمير العدو بصواريخه وقذائفه هو ذاته وهو الامر الذي اعترفت به قيادة العدو العديد من المرات بينما اخفت هذه الحقيقة مرات اخرى معللة حدوث ذلك بما يسمى بالنيران الصديقة التي طالما كانت مثارا للضحك وسخرية العديد من وسائل الاعلام الاوروبية لاسيما خلال الاسابيع الاولى من الحرب في عام 2003.

ب - منظومة امواج الميكروويف للسيطرة والتحكم على الذخائر الموجهة بالأقمار الصناعية :

مع بداية الالفية الثالثة فقد تمكن الخبراء العراقيين من ابتكار منظومة اخرى للسيطرة والتحكم بذخائر العدو الذكية الموجهة بالأقمار الصناعية ولكنها تعتمد على تقنية الميكروويف بدلا عن الموجات الفوق صوتية. حيث طور خبراء الحرب الالكترونية تقنية خاصة تستخدم موجات الميكروويف - القدرة المستمرة (Power.Microwaves.Continual.CPM) لتضليل القنابل الذكية من فئة قذائف الهجوم المباشر المشتركة (JADM) التي تطلقها الطائرات الامريكية ويتم توجيهها نحو اهدافها بالموجات الفوق صوتية التي تصدرها مجموعة اقمار نافستار الامريكية بموجب نظام تحديد المواقع العالمي (GPS).

ونتيجة لاستخدام القوات العراقية لأجهزة تشويش على الاقمار الصناعية التابعة لوزارة الدفاع الامريكية البنتاغون، وعلى ذخائر العدو الامريكي المنزلقة على اشعة الليزر، وعلى اجهزة الرادار والاتصالات في الجيش الامريكي والبريطاني، فقد اعلن قيادات العدو ومسؤوليه عن وقوع العديد من الخسائر في صفوف قواتها الغازية نتيجة ما اسمته بالنيران الصديقة. وهو المصطلح الذي دائما تكرر خلال الاسابيع الثلاثة الاولى من غزو العراق وكان مبعثا لسخرية القارة الاوروبية والتي كان قد وصفتها الولايات المتحدة بالقارة العجوز نكاية بالأوروبيين بسبب رفضهم المشاركة في العدوان على العراق. وقد نشرموقع الجزيرة نت يوم 2003/4/6 مقالا بعنوان ((أوروبا تسخر بالنكتة من الحرب على العراق)) جاء فيه :

((ماذا نسمي الهدف الذي يضعه فريق في مرماه في مباريات كرة القـدم؟.. مقـدم الـبرامج التلفزيونية الألماني هارالد شميدت يرد على هذا السؤال كل مساء "إنها نيران صديقة", وهو التعبير الذي تستخدمه القوات الأميركية والبريطانية للحديث عن الجنـود الـذين يـسقطون بنيران زملائهم.

وهذا ليس في ألمانيا وحدها بل في كل أوروبا كما هو الحـال في جميـع أنحـاء العـالم، حيـث واكبت النكتة السياسية جنبا إلى جنب وسائل الإعلام تطورات الحرب على العراق. واتسمت هذه النكات بقدر كبير من السخرية خاصة من الـزعيمين الأمـيركي جـورج بـوش والبريطـاني توني بلير اللذين يقودان الحرب على العراق.

ففـي اليونـان حيـث مـا زال كثـيرون يـذكرون دعـم الولايـات المتحـدة للحكـم الـدكتاتوري العسكري هناك (1967-1974)، يتناقـل الـسكان نكتـة تقـول إن "طـائرة تقـل بـوش وبلـير تحطمت , فمن يكون الناجي من الحادث؟" والجواب هو "العالم بأسره".

ويسخر الروس أيضا من سير المعارك والصعوبات التي تواجه القـوات الغازيـة. ويقولـون إن "التحالف الأميركي البريطاني أعلـن سـيطرته عـلى أم قـصر وهـي رابـع أم قـصر ينجحـون في الاستيلاء عليها منذ بداية الحرب".

أمـا صـحيفة إزفـستيا الروسـية فقـد انتهـزت فرصـة الأول مـن أبريـل نيـسان لتنـشر عـلى صـفحتها الأولى نحـو ثلاثـين نكتـة عـن العـراق مـن بينهـا أن الـرئيس العراقـي

صدام حسين أعلن إسقاط طائرة بريطانية , لكن بوش ينفي ويؤكد أن الأميركيين هم الـذين أسقطوها.

وعودة إلى مقدم البرامج الألماني شميدت الذي يشرح لمـاذا تـأخر الأميركيـون في الوصـول إلى مشارف بغداد فيقول إن القوات الأميركية تأخرت وكان يمكن أن تبلغ هـذه المواقـع بـسرعة أكبر , ذلك "لأن CNN اضطرت لإعادة تصوير المشاهد مرات عدة".

المراجع

- موسوعة المقاتل الإلكترونية، سمو الأمير خالد بن سلطان بن عبدالعزيز 2015.
- الحرب الألكترونية، كريم حميده، مقالات 2012.
- إسرائيل والحرب الإلكترونية، شموئيل ايفن ودافيد بن سيمان، معهد دراسات الأمن القومي -إسرائيل. 2011.
- "الحرب الإلكترونية" - جبهة جديدة ضد "داعش". موقع دوتش فيلي الألماني بالعربية. 2014.
- منظومات الحرب الالكترونية، مدونة الرفيق رأفت علي. 2013
- الحرب الالكترونية تساهم في حماية القوات الامريكية في العراق. مجلة السوسنة 2010.
- الحرب الإلكترونية على إسرائيل : الأبعاد و الدلالات، مصطفى الديماني، موقع الحقيقة 2013.
- موقع الجزيرة الإخباري.
- صحيفة القبس الكويتية

الفهرس

/تم بحمد الـلـه/



دار الجـــــنادرية للنشر
الأردن - عمـــــان
تـــلفاكـــس ٦٤٧٧٨٧٧٠
وال ٠٧٩٦٢٩٦٥١٤
٥ عمـــان ١١١٥٢
dar_jana